Lars Magnusson (lm222mc - Linnaeus University)
4DV505 – Current Topics within Computer Science
Linnaeus University, Dept. Of Computer Science
(2016-04-22)

Integration as Secure IT Architecture Driver

Lars Magnusson, M.Sc. CISSP ITIL

Paper

April 22, 2016

Intentionally empty.

Content

Author's Comment

This paper is the author's first academic paper since 1984, since when presenting my M.Sc. Paper, "Seismic interpretation of Tertiary Sequence, Block 6507/12, Northern North Sea" at Department of Geology, Chalmers School of Civil Engineering, an international master in Petroleum Exploration. Though having written strategy papers, policy documents, project, operations and systems documentations, as well as procurement specifications and agreements for the last 30 years, again adapting to the academic standard has not been easy.

To use Wikipedia's editor team's sometime harsh valuations of entries, this paper suffers from both subjective comments as "weasel words".

However, it is important to recognize that the driver for this paper did not come out of a need of an academic process, it is a direct result of trying to map today's Information Security situation to a practical experience, using the academic process as an enabler for further work. To take those 30 years' experience of solving complex IT issues, compare to what others written the last decade and try to extrapolate some possible and realistic architectural solutions, needed to protect us from the increasing threat of cyber criminality.

Abstract

As per 2015 the international IT market has seen a substantial shift in the status of IT security. A Symantec representative declared already in May 2014, "Antivirus is dead", thereby pointing out what the Internet Information Security community ever more frequently experienced; that the "Bad Guys" is getting better than the "Good Guys". More professional and with more resources, they mount attacks that is more successful than only a couple of years ago.

As discussed at (ISC)2 2015 SecureScandinavia event, May 2015, the current time to achieve a breach is approximately 5 hours, while time of discovery at an average is over 200 days.

200 days to wreak havoc with the victim's ITC environment or even worse, using the victim as stepping stone to other victims. Much like when the US consumer chain Target was hacked via their climate control vendor. Something leading to a loss of 40 million customers' personal and credit card data and forcing to a settlement of $10 million.

We need new Information Security paradigms, allowing us to attack the problem in new ways, mitigating the current inherited limitations, we daily suffer from in our ITC environments. For it is clear, the quality control of software solutions is under par. We need to be inspired by the manufacturing industry, how to improve both development processes as well as software quality. For fact is, most of the current top software culprits has been well known for over a decade, yearly listed as SANS Top 25 Vulnerabilities and OWASP Top 10 Vulnerabilities.

But, since processes and programing is created by humans, we cannot expect the faulty processes or code to be corrected short term. The problem solutions have to include mitigating current processes and solutions, thus creating substantial "speed bumps" for the perpetrator, making the own organization less appetizing as a target.

This done, using alternate architectural solutions, where limiting non-essential access, "deny all" must be the key component. This paper is to look at some possibilities already available, using modern IT architectural components as "onion" network (aka. not Tor), messaging hubs and better process support.

Terminology

Terminology and shortenings used in this paper.

API	Application Programming Interface
BaselIII (3)	Basel Agreement-International financial control
DBMS	Database Management System
CEO	Chief Executive officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COO	Chief Operations Officer
CSO	Chief Security Officer
CSA	Cloud Security Alliance
DDoS	Denial of Services attack
DMV	National Department of Motor Vehicles
EDI	Electronic Data Exchange
EMF	Electro Magnetic Field around factory equipment
ENISA	EU Agency for Network and Information Security
FW	Firewall
HR	Human Resources
(ISC)2	Information Security Certification
ICT	Information and Communication Technology
IDS	Intrusion Detection System (Host=HIDS/Network=NIDS)
Info	Information
Infosec	Information Security
ISACA	Information Systems Audit and Control Association
IT	Information Technology
IoT	Internet of Things
IP	Internet Protocol, TCP/IP network stack base
IPS	Intrusion Protection System (Host=HIPS/Network=NIPS)
IPsec	Network encryption protocol, IPv6, also used in IPv4
IPv4	Version 4 of IP, addresses like 162.198.0.1
IPv6	Version 6 of IP, addresses like fdda:5cc1:23:4::1f
ISO	Information Security Officer
MMM team	Mythical Man Month organized development team
MOM	Message-oriented middleware
MSc	Master degree of Science
NAS	Network Attached Storage
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OWASP	Open Web Application Security Project
PIO	Process Information Officer(BPM area IT manager)
PhD	Doctor degree of Philosophy
PLC	Programmable Logic Controller - robot/line sys
Ransomware	Program encrypting accessible files to extort victims
Red Team	A team challenging an installation or change requests
SAN	Storage Area Network
SANS	SANS Institute
SAP	A German Business Software Integrator
SCADA	Supervisory Control And Data Acquisition
SDN	Software Defined Networks

SOX	Sarbanes-Oxley Act, US, financial control
SSL	Secure Socket Layer - depreciated for TLS
TCP	Transmission Control Protocol - part of TCP/IP
TIO	Technical Infrastructure Officer
TLS	A newer more resilient version of SSL, Transport Layer Security
Trojans	Software having clandestine components
UDP	User Datagram Protocol - part of TCP/IP
USB	Universal Serial Bus - a standardized appliance
API	Application Programmable Interface
VLAN	Virtual network - simulating a network
VPN	Virtual Private Network - encrypted lines
WLAN	Wireless network
Zero Day	Use of Information Security exploits, not know beforehand

1. Problem Introduction

Passing into 2015 the international IT market started to experience a substantial shift within the operative status of ITC security. A Symantec Vice President stated in May 2014 that "Antivirus is dead" (Chacos, 2014, Whittaker, 2014), pointing out what the Internet Information Security community frequently experienced the last couple of years. That the "Bad Guys" is getting better than the "Good Guys". Becoming more professional and with far better resources. Thus able to mount attacks far more successful than seen 4-5 years ago (Hart, 2015, Hansen, 2015).

With the time to create a breach gone down to an average of 5 hours, time to discovery still average +200 days. Ample time for the perpetrator to analyze and utilize the victim's IT environment, like how the Target attack in 2014 unfolded (Riley & Pagliery, 2015), or as noted in 2005 by a US automotive CISO, at the weekly global CISO Core Team meeting, “At any given time, we have at least one, maybe several unwanted visitors”. The automotive team got better fending these “lurkers” off during 2005-2009, but as the in this paper included Automotive and Manufacturing cases shows, large modern, IT integrated organizations are per design vulnerable.

Also noted by several speakers at the 2015 SecureScandinavia event, today's hackers are organized as research organizations, not as traditional hackers; employing CS researchers, like PhD’s and MSc’s. Fully qualified, well paid computer scientists with pension plans, child care, holidays and other fringe benefits. Creating a completely new breed of IT criminals, IT professionals (Hart, 2015, Hansen, 2015). People studying new software packages and bug reports out from a scientific perspective, attacking with a vigilance, few in the opposition can compete with.

Consequence: FBI reported early 2015 that, as a low estimate, cyber-crime cost was at minimum $800Mn in 2014 (FBI, 2015). 2014 World Economic Forum and McKinsey published a report that estimated that global cyber-crime protections measures in 2020 likely will reach some $3 Trillion, seriously affecting the global economic growth (WEF, 2014). Affecting both public organizations as corporations and individuals everywhere, due to increased spending to avert cyber criminality.

Since 2014 we also seen a strong increase in the number of IT extortion cases, with several Danish and Swedish municipalities, like Stockholm Läns Landsting, being hit with ransomware (Malm 2015, Møllerhøj 2015, Satz 2015). The author has own experience of being targeted 7 times between Jan 1 and March 15, 2016.

An old maxim in the Information Security community, learned early on in the game, is that around 70% of all IT crimes is internal and the rest is external. That is, we are more likely to have the criminal at next desk, rather than someone being in another country (Shein, 2015). However, with the current development of loss of value, if external criminality yet hasn't surpassed the value of internal crimes, it soon will. We also have to see beyond this, for internals will more frequent likely work in conjunction with external perpetrators.

Why this problem?

As demonstrated already in the 1990: ies by Nike, concentrating on design and sales, procuring manufacturing capacity (Donaghu & Barff, 1990), data has become a multi-dimensional commodity, not only internally, but also in the interface between customers and vendors (Antilla et.al, 2004). One department’s data, is the raw material of another. The time when one department could talk of “my data” is long gone (Magnusson, 2013(1)). At the same time, the same data is crucial for our survival, requiring new types of protection as it floats around.

We will never become safe, IT is technology and as Murphy's Law says; “If anything can go wrong, it will” (Murphy, 1949). And as most of us has experienced, at demonstrations or lectures, it does some day and then at the most inconvenient time. We will be hacked, but we must try to make the cost of hacking us higher than hacking the neighbor. Therefore, the overall IT system architecture and ITC processes need to become better and more resilient to attacks. We need to put more money into our cyber defense. And if we can't fund it alone, we need to cooperate with others, about commonly acquired improved solutions. Public sector being a prime candidate for such cooperation.

We also need to integrate information security processes more naturally, allowing to define the security risk picture, before any functional demands in our procurements. We also need the leadership to understand that it is they that have the legal and ultimate responsibility, not the CIO (Kotulica & Clark, 2003; Antilla et.al, 2004; Lindström, 2009; Soomro, Shah & Ahmed, 2015).

With the current still heavy dependency on legacy systems, the only way to do this is to review our total information architecture. To realize that we no longer have isolated islands of systems, but a complex interaction between all our systems (Magnusson, 2013(1); Soomro, Shah & Ahmed, 2015). We need to identify and break down the actual data flow involved, rebuilding the architecture into an interchangeable solution, driven by the data flows, where communication and access is protected with proper access control and communication encryption (Bossert et.al., 2015). Neither being rocket science, already supported by most PKI systems and network technologies like IPv6/IPsec.

We just need to implement the solutions. Particular today, when any organization, private as public, need to react more expediently on accelerating market/society changes. ITC need to support ever more agile changes and do it with better security (Bossert et. al., 2015). This independent if supporting internal, outsourced or cloud solutions.

We need to look at Information Security from a holistic perspective, something evolving the last couple of years, how to match security with the business processes (Badr et.al., 2011), including the necessary process side (Magnusson, 2014).

This paper is based on the practitioners need of looking at these ideas, iterate them into by audits proven solutions, using agile system integration and messaging as tools to evolve a necessary flexible, security inclined and data oriented architecture (Antilla et.al, 2004; Talla & Valverde, 2011; Bossert et.al, 2015) out from our existing legacy solutions.

1.1 Paper Introduction

Information Security have traditionally been something added to information solutions as a last stage, a backpack to the systems it is to protect or as a hindsight (Spafford, 2009). This do have improved some since mid-2000, like protective access controls as Microsoft Active Directory or similar products, e-mail protection or one-time passwords key fobs like SecurID and Ubikey.

At the same time, we seen some serious laxation's, like reduced scanning of e-mail for possible executable attachments, such as was done in the wake of the late 1990: ies/early 2000 e-mail viruses like "Anna Kourikova", Sircam and Melissa. It has recently been reported that both Word Macro viruses as JavaScript viruses is back (Donohue,2015, Mendrez, 2015).

Add to this a number of ransomware attacks, tweaking receivers into running a link to a down-loadable program, the victim believing to be a confirmation of waiting postal package (Malm 2015), as well as emergence of new innovative attack pattern, socialized attack patterns, using methods of social disguises, cultural ploys and psychological ruses. To get the targeted users to unwittingly assist the hackers to access our computer systems and networks (Abraham S., Chengalur-Smith I., 2010).

All creating economic and practical issues, fending off these attacks. We need a new Information Security paradigm, both regarding processes as architectural, not to again repeat the "same ol', same ol'" we've done for the last 15 years, perimeter control and antivirus.

We need to build sectional and functional defenses, placing the critical resources into protective zones, simplifying the IT architecture, not to trip over our own legs (Bossert, Richter & Weinberg, 2015).

We are not talking new technology. Particular defense contractors and military have used related methods to secure sensitive system and data from the general surroundings since 1980: ies. Using both air gap (non-connected networks/-systems) as well as virtual access via shielded, encrypted VPN network into virtual PC instances, inside a secure network and with lesser access rights. Something also been used within Automotive, to support external development teams (Magnusson, 2010).

Previously much of this has been a technical challenge, like multiple data centers, requirement of nearness to productions systems (factories/hospitals), fractionated localization, poor network capacity, choked networks etc. But with the event of virtual computing, contextual firewalls, NIPS/HIPS, Gigabit, VPN, IPsec, and Software Defined Networks (SDN), it is possible building both stable, sectioned secure wide area as well as end-to-end networks, shielded from any actual physical network structure employed (Rouiller, 2003; Leischner & Tews, 2007). Today hardly no-one rents a physical private line to connect two sites/organizations, it is mostly done by creating an encrypted VPN over Internet, using IPsec.

Spring 1999, at a lecture at Stockholm IT Fair, a team from Volvo showed a surprised audience, better up-time with Internet based VPN than with leased lines, 98% to the latter's 90%. A figure now vastly improved, in 2005 allowing the US mother to the local Swedish company in Case 4.1 to support the mother's whole European operation from Turkey and Spain to Russian Republic, with Internet based VPN connections to vendors, requesting this functionality. A solution architected much according to the above referred guidelines, by the author (Magnusson, 2010).

Due to current extended threatscape, the guiding protection concept must therefore to be to better follow existing, well known and accepted "Best Practices", limiting access to involved systems by using methods of secure networks and protocols limitations. Block all and allow only business motivated traffic (Heidelberg, 2007; Bossert et.al., 2015). One reason not yet using this internally, has often been the internal communication "maze" of ad-hoc implemented system connections. It becomes an operational risk to block traffic, since our system architecture understanding to often is incomplete (Kindervag, 2012).

Locking down non-critical protocols and network routing will be discussed in "4.1 Case Automotive". The guiding principle was using protective layering and reduce communication patterns. If individual access to protected systems was needed, it was expedited via either a web service gateway, reached through an inner perimeter secure web proxy or if terminal access, done via router filters for ssh.

Reducing mixed inter-system communication is crucial. As found in both Case 4.1 and Case 4.2, system connections grow organically, data from one system suddenly needed by another. The system owners and managers discusses a connection between their systems and the admins set it up. Far too often, as proved by most audit records, without proper change review. Even using ITIL based approval/change systems (Weil, 2010; Magnusson, 2010, Magnusson, 2011(2)), in the haste of solving critical business needs, many such connections never get proper documentation and later to become a security and/or audit nightmare when the involved personnel have moved on. Still hopefully found in an audit, before getting exploited.

As experienced in Case 4.1, when a global remediation of ftp usage, forced by implementing the Sarbanes-Oxley audit process (SOX). A FTP based messaging system, handling some 50.000 messages a day between some 20 core servers on 9 OS platforms, stopped a local Swedish remediation cold. To this messaging system; another ca 1-2.000 daily automatic ftp data transfers was made locally or to/from other divisions around the world, outside the messaging system.

The lesson learned was, that however good your ITIL processes and CMDB is, in critical situations the involved personnel becomes human and pushes all processes aside. The employees need a liability incentive to handle their changes in time, to follow the agreed change process and approvals. This case later included an effort to replace the haphazardly designed direct system connections with a modern central data exchange hub. Both to allow reuse of data, where a single input could be distributed to multiple receivers, as well as to limit number of communications protocols needed, allowing a widened protocol blocking.

Another driver was to downsize and simplify a previous global manufacturing IT support scope, to a more prudent for a small local automotive brand. From a security point of view, having 100:ds of connections using insecure protocols like MS-SQL or SMB, as well as PLC and SCADA system communication, reporting back to production control systems, the network was hard to filter.

As discussed 2010 within the ITC team at Case 4.1, we also looked at integrating systems, not through building monolithic systems, but via flexible modularity, easily supporting future business changes. Think UNIX Tools, (Bossert et.al., 2015).

The intention with this paper is to see how those ideas around processing, communication control and integration tools can improve and support modern Information Security.

1.2 Problem area

The general problem area is that we today have more proficient cyber criminals, far more knowledgeable than their targets own ITC personnel. To this, we have the present drive toward more complex, interacting ITC environments; data becoming an internal commodity, changing in nearly every nook and cranny within the organization. Where the target organizations seem to be losing their overview of their ITC operations (ref. Case 4.2). We currently see many local business managers repeating their mid-1990: ies counterparts failing local PC server strategies, but now via procuring cloud or other external services without any consideration how these will match the overall strategy or data flow. Often due to lack of confidence in the ITC team.

One important driver for this is financial savings in operations. It is well-known that companies like Google, Facebook, Amazon, Microsoft and Salesforce have low IT personnel count per server, one person maybe handling 200-500 servers; Microsoft even declaring 1000-2000 servers per administrator; though 150 servers being regarded more realistic (Miller, 2009; Clark, 2010). Operations figures our managers hear about at convents and expects to copy.

But staffing of this nature is based on a uniform base architecture. A treat these behemoths exhibits, unified server and network platforms, used by millions of customers, each of those maybe only handling 3-4 virtual instances.

In one respect, we're back to Henry Ford's 1920 "theorem" about automobiles; "Any customer can have a car painted any color that he wants, so long as it is black" (Ford & Crowther, 1922), When doing large volumes, we can do any work and products cheaper, but when buying a Bugatti Veyron or a Koenigsegg or even a Saab, it will cost. Due to their limited product volume and thus relative more complex manual assembly. This has implications for normal, multifaceted organizations, supporting smaller heterogeneous ITC environments. If thinning operations, we lose the competence base needed to expertly counter-act this new type of cyber criminality.

We therefore have to have a modified angle of approach; deny all until needed, simplify the overall architecture, to make base environment resilient to basic attacks. In principal, by applying the ideas of Richard Saul Wurman (Wurman, 1997), about information architecture as a larger concept, than isolated data models per systems, normally used in ITC projects. By envisioning a total data landscape, we can review our info systems out from the same perspective as Nike did (Donaghu & Barff, 1990).

Through adopting the value of the total information, we can get relevant metrics even on processes like Information Security (Tashi & Ghernaouti-Hélie, 2007). To being able to create a full data-flow model, envisioning risks, new ways of processing, security data during transfers and to see how external sources will affect our ownership control and thus improve understanding of our legal responsibilities and liabilities regarding our data. A legal aspect most leadership teams currently do not realize.

As seen, with among other cases, the US Target attack (Riley, Pagliery, 2015), such un-visioned legal liabilities can cause substantial damage to the financial bottom line. We need to strengthen the control over our data, in order to maintain these legal responsibilities (Badr et.al, 2011). Something to be noted in the yearly risk assessments.

To make a "real world" analog regarding maintaining control; in 1933 the International Court of den Hague, in the decision of the case Norway vs. Denmark, regarding North-East Greenland sovereignty. The court ordered Denmark to actively show their presence in North-

East Greenland, if to maintain the declared sovereignty (Forsvaret, 2016; Nilsson, 1978). Something later debated and copied in several other cases, as the Falklands, South Georgia, Kerguelen and other, mostly non permanently inhabited, geographic territories. The court established, no active control, no ownership.

IT is not territories, but as seen in contracts and conditions between users and Internet services during the last decade, many services have some writing to allow extensive data mining usage, such as Google Analytics or Facebook ad positioning (Google, 2016; Facebook, 2016). But we also seen cases where a service simply has peeked into data, like Dropbox, for undisclosed purposes (Kirk, 2013; Luckerson, 2014). Cases not unique.

To summarize, the history thus makes a case for the leadership to study and question, if the organization's data ownership need to be handled in similar ways as the 1933 International Court decision argues. That any organization need to prove it has a controlled ownership and management control of its data, independent where it is; in-house or at an outside contracted service. And if the latter, proving, through a clear and unambiguous contract, that it has established a legally valid control, even when the contracted service is handling the data (Lindström et.al., 2015). Such a view also has consequences for employees, that often in Ad Hoc and non-contracted manner uses outside services (like Dropbox). Usage that can render the leadership liable to any service's misuse of the transferred data.

A possible consequence could be, that a leakage of data affects a private incorporated organization's stock evaluation or that restricted data (primarily privacy data) is publicized in an uncontrolled and unlawful way, both making the leadership liable. A typical example the author been forced to handle, has been EU regulated data privacy information or according to the even harder German Bundesverfassungsgericht (Federal Constitutional Court) regulation regarding said data.

Unfortunately, we are not there yet, there is lack of research into several of the topic areas; leadership liability of involuntary leaked data through external services; maintaining control when data physically left the internal network, better, more security innovative architectural solutions and support for the increasing need to replace the 1980: ies/1990: ies and early 2000 legacy systems, not built to support current standards or requirements. And designing new data governance architectures, based on the data-flows no longer limited to the local organization, but the total environment. We need improved evaluations, including financials, to our legal status and risk charts, to improve these processes (Bossert et.al, 2015; Stafford, 2009).

However, this paper has a limited scope, looking primarily at three <u>strategic</u> aspects;

a. The use of sealed network segments to isolate sensitive, hard to protect and often legacy systems, funneling communication in a way increasing information security,

b. use of a messaging function to decoupling direct system-to-system communication, thereby simplifying number of needed protocols and communication paths, thus supporting remediation by allowing step-wise system exchange/modifications/mitigations with less disruption of operations, than traditional upgrade methods and lastly

c. the needed processes to keep system and change documentation to par, to improve ITIL and ISO 27000 and support audits.

1.3 Knowledge gaps

As noted, a large part of this paper is based on the author's activities as Technical Information Security Manager, Information Security Officer and later as Senior Security Consultant/Security Services Developer between 1999 and 2015.

Work that included to re-mediate and mitigate information security problems within "Case 4.1" and later as consultant, particular as scope planner for a Swedish global technological manufacturing customer, "Case 4.2", used here as test cases. Both entities had grown via procuring competition, thus creating hardware and software zoos, with largely incompatible IT systems. During which timeline, data integration accelerated due to new manufacturing methods, pushed via operative integration; such as through new PLC or SCADA system solutions, not seldom operated from equipment manufacturers remote operating centers. Siemens and Dürr being two important vendors, both with large operations centers in Germany.

In 2008, the author architected Dürr's access to a car body shop line at a Swedish daughter of a US Automotive firm (ref. Case 4.1). Dürr accessing through a regulated VLAN and IPsec access into a manufacturing line perimeter router with inverted firewall, allowing vendor PLC or SCADA specialist to maintaining the line, not seeing the rest of the factory, while the local technicians still could control the data models used and the line flow control. When later audited, the solution got full approval in an SOX audit.

However, due to often imbricated implementations on site, this type of integration often drives operations cost. In Case 4.1, Dürr, Siemens and two local Swedish solutions was intertwined in the same factory. No discussion about coordinating technology, the manufacturing division saw it as separate line problems, not ITC problems. While still demanding ITC to solve frequently appearing issues. Architectures driving insecure solutions. However, due to the Stuxnet Trojan, Siemens and Dürr learned from all bad public relations and improved their communication processes.

Most solution firms working these problems, tries to solve customers' business integration issues by building large monolithic integration platforms. Though the underlying idea is sound, migrating a "living" environment over to such platforms is problematic and costly. We yearly see articles about substantial project overruns, even threatening the customer's survival, as happened for Swedish Bröderna Nelsons Fröer, ending up with a SAP installation costing 1/3 of the yearly budget (Andersson, 2001). Though not an Information Security factor, it is a substantial risk factor, also affecting Information Security, when the project tries to save the day and start taking shortcuts. Clear is, we need better methods, that holistic develops and mitigates legacy architecture without compromising security, but improve it per design (James, 1996; Antilla et.al, 2004; Badr et.al, 2011).

Though there are some studies within integration vs. security, primarily due to the growing usage of cloud services, this author has been unable to discover more than a few studies that direct addresses the complete IT chain, including how to maintain legal ownership and responsibility of the data processed and allows for a modularity to keep up with business changes. We see a growing and important gap there, where several authors question our current evolution (Spafford, 2009, Kindervag, 2012; Bossert et.al., 2015).

As mentioned in the previous section, this paper intends to only look at three factors involved in the total problem complex, trying to address some of the limitation currently dominating this area of IT. The hope is to also inspire others to once again look at the system maintenance and security processes in conjunction with data management, rather than the current trend of focusing on system management. The latter is still needed, but as previous said, we need to adapt to a new data oriented world.

1.4 Research question, objectives and delimitations

The initial research question is larger than the scope of this paper, how to realign information security to secure data in an expanding distributed world. A topic area where we currently are strongly depending on outsourcing and cloud vendors, as well as other service providers word, that our data is secure (Google, 2016; Facebook, 2016).

Unfortunately, we each year see a number of cases proving something else, like previous mentioned Target incident (Riley & Pagliery, 2015), but also attacks against Home Depot and Goodwill.org (Hardekopf, 2015) and others (Soomro, Shah & Ahmed,2016) or like Facebook and Dropbox looking at customer data (Kirk, 2013; Luckerson, 2014).

Swedish IIS.se's Chief Security Officer, Anne-Marie Lövinder Eklund have at several occasions during 2014-15 voiced the view that at least public organizations in Sweden shall be required to alert any data breaches to the Swedish governmental security agency, MSB.se. Reason is two-way, to inform citizens about pending risks regarding they privacy data, as well as to build an incident database, capable of driving "Best Practices" among at least public IT. OWASP Sweden, Cloud Sweden and CSA Sweden have each had a number of open projects addressing this, e.g. practices already existing, not needing to be developed (OWASP, 2016; CloudSweden, 2016; CSA, 2016). However, we need better process support for that development.

We need research, not only looking into the processes and architectures, but how data really is transported around (Bandyopadhyay, 2010). Internally as externally. Very often Web Services, protected by TLS is used, but TLS as only defense can be debated, particular as it can be attacked via "man -in-the-middle"-attacks or XSS, cross-site-scripting, injecting clandestine servers into the network flow. Clandestine servers responding with valid TLS encryption, reading all in clear text, even manipulating data, before forwarding to the correct destination (Raza & Alli, 2011; OWASP, 2013).

We need to improve resilient to such attacks and understand the flows, so we can evaluate the risks of data being exposed during its traversal through our system landscape. Risks addressed by both IETF Security Chair (via public address during the IETF-75 Stockholm meeting, 2009) as Forrester Research's Zero Trust initiative (Kindervag et.al., 2011; Kindervag, 2012) and others (Bandyopadhyay, 2010). This led to the initial question; "how to make data securer".

Traditionally IT security been regarded as access control and network perimeter protection (Cheswick & Bellowin, 1994; Garfinkel & Spafford, 1996, Spafford, 2009), but with time, available exploits and new attack vectors has forced new security solutions. Tools like NIDS/HIDS, which now is felt not to handle an evolved situation; as debated by among others (Behl et.al., 2012), (Zimmerman, 2014) and (Raza & Alli, 2013). The consequences of the increased use of Trojans, DDOS attacks and ransomware, how do we fend of such attacks.

Maybe we in a possible near future will see the use of IPsec enabled end-to-end networks based on Software Defined Networks (SDN) as protective effort (Abad-Carrascosa et.al., 2015). Building nearly Ad Hoc networks, able to support managed system-to-system secure communication. But already today it is possible to implement subsets of such "future mode of operation" solutions, like fencing of insecure protocols to/from secure core zones, thereby creating layered networking structures, the first stage to fend of the "the Wiley Hacker" (Cheswick & Bellowin, 1994). All technology is there, but how do we use it?

The first option would, managed, secure SDN networks likely by all conveniences to be the most secure, but requires major larger change projects, going per related server groups, communication-wise. A project in need of massive PKI support for IPsec key distribution.

The latter option is possible to instigate in a stepwise implementation process, reviewing protocols per server groups / network segments. As experienced through Case 4.1, such a protocol by protocol remediation is possible to do without breaking day-to-day operations. Take seven months, due to identify all communications, but very doable. Though only ftp and telnet was remediated in this case. By including a sftp/ftp conversion gate at the core network perimeter, partly simulating the idea of a "Common Bus Communication", a unified, but restricted data API, requiring encrypted access (Bossert et.al., 2015), it became clear that a general messaging solution would greatly improve on the connection pattern, strengthening against attacks, since the core servers had a "block all" for the insecure protocols, as well as the messaging function having security analyze capabilities, at that time NIDS.

Due to a bankruptcy late 2011, wider tests never was implemented, but was later at another employer developed as a study concept model for building secure "onion" networking, "Information Security Onion Operations Model" (ISOOM). In the end it was decided not to fit into the organization's product portfolio.

Before 2010, an architecture like ISOOM would have raised capacity concerns, but today we have system and network solutions handling millions of requests. By adding a standardized multi-protocol messenger system, remediation of systems could be done simpler, analyzing the data flow for each system, migrating their data flow one by one to the hub. At the same time, "user" access will be limited, primarily web functions or ssh, no "Man-in-the-Middle". With limiting traversing traffic patterns, other attacks are easier to fend off. Later, when encrypted SDN will be more readily available, we also are likely to improve DDoS resilience (Jonker & Sperotti, 2015; Lim et.al, 2014).

However, the paper limitation at hand being the three sub-issues; how logistically securing data flow by using the ISOOM model, the effect of using a messaging hub as an active security mitigation factor and look at an improved, administrative inclined, user centric approval system.

2. Research Process

2.1 The research process for this paper

This paper is implicitly handling an area that currently seems to be seriously neglected, both within academia as in operations; system management. Yes, we have ITIL, ISO27000 and other methods, but their relation to today's more connected IT environments and a higher IT threat profile is limited. Previously mentioned network and communication limitations and risks could present a far better standing in audits and other surveys, if we really used the tools available.

The author's communicated with several Swedish universities, reviewing their involvement in the topic area. Result was, there is currently only limited research efforts within operative ITC processes in Sweden. Some research was done at Linköping University up to 2014, but due to researchers moving on, nothing is done there today. Contacts with Lund, Karlskrona, Linneus, Luleå and Gothenburg University indicates that neither of these have any programs on-going within this, historically traditional Swedish research area, going back to the late 1970: ies.

At that time, through initiatives by Svenska Samfundet för Informationsbehandling, Riksdataförbundet and in the end of 1980: ies with Swedish Computer Society's "System-förvaltningshandbok". The latter very similar to the contemporary British Standard 15000 (ITIL).

But with the event of ITIL, the topic seems to have become an academic "not invented here". With ITIL said to be slipping behind today's distributed and connected environments, some mitigative processes can be found in ISO27000 (Sheikhpour & Modiri). But still, IT is a moving target and standards is always behind, but the processes must adapt, therefore some effort has been allocated in this paper to review some of this.

Looking further at the current technology, as discussed last year (2015) within Swedish Network User Society (snus.se), Internet of Things (IoT) do not stand up to any reasonable security best practice, creating even larger risks. This said to be due to being primarily developed by network oriented people (Kindervag, 2012), but mostly using network protocols micro stacks lacking most security and management feature. Something many, like SNUS and IETF Security Chair, now frequently warns for.

With a healthy research, ITIL and other management processes can push for today well acknowledge "Best Practice" mediation and mitigation solutions (Christey, 2011; OWASP, 2013), demanding producers of new features to adhere to sane processes and solutions, allowing the new features not to become a risk factor, but so far this has been a non-event.

Unfortunately, having been in ITC operations for +30 years, I must admit that I never met a CEO/CIO, that with self-preservation would allow their ITC management group to put time on such "un-productive" efforts. Same with software creators. Professor Gene Spafford at Purdue have been very adamant in his criticism, regarding lack of responsibility (Spafford, 2009). The competitiveness of today's corporate and public organizational environments only allows for including cost-effective COTS solutions, not to study and implement better methodologies.

After reviewing referred articles and books, finding limited information relating to this paper's primary topic area, securing the data flow, the author has chosen to "go back to the roots".

That is, revive former work within Automotive, as well as using subsequent work at the succeeding employer, a Finnish-Swedish consultancy firm. Work later evolving into the earlier referred “Information Security Onion Operations Model” (ISOOM) and an improved ITIL management process, with a clearer approval chain. Trying to validate or refute my findings.

To conclude, apart from Forresters Zero Trust initiative (Kindervag, 2012), Bossert’s suggestions (Bossert et al., 2015) and Case 4.1, there currently only found limited support for ISSOM-like operations models, including using messaging as an integration and security enabler. But as indirectly indicated in a number of reviewed texts (Talla & Valverde, 2011; Joshi, 2007; Kendritas, 2013, Mulholland, 2015), we cannot ignore that new requirements soon will drive new views of solutions within the topic area. As noted before, this is an area in desperate need of hard research, to counteract the last 4-5 years’ expansion and re-innovation of cyber criminality.

2.2 Evaluation model applied

Due to the scope of the paper, currently lacking current relevant “up-to-date” cases and with limited research resources, much due to the author not being a full curriculum student, the work for this paper has been forced to extrapolate two previous work cases as my solution models.

Additional to this, no particular evaluation model beside general business “Best Practice”, based on ISACA, SANS, OWASP, CSA and others Best Practice processes, has been used as base for this work. Referred to, but not included is the author’s work for Sollentuna Municipal Council (Magnusson & Salomé, 2012), regarding a municipal Cloud Service Best Practice, as well as ideas presented via Forresters Zero Trust initiative (Kindervag et.al., 2011; Kindervag, 2012) and Bossert’s related ideas of securing modern data flows (Bossert et.al., 2015).

This is a clear and unfortunate limitation, but intention was to see if this work could be foundation for succeeding extended work.

2.3 Approach used for literature studies and cases

This study is based on material extracted from course literature from Linneus University course IK501, articles and reports required from LNU Library as well as Lnu’s service, OneSearch.

This material is supplemented with work material and the author’s empirical experience from a global US Automotive corporation, as well as it’s now defunct Swedish daughter and their ITC vendors. To this, some own published articles in US and Swedish press has been reused. All material is listed in the reference section.

Basis for the literature searches has been Information Security in conjunction with System Integration and Information Architecture as well as securing the network. Some 150 articles and books has been evaluated, with about 90 included as reference for this work. Of the latter ca 20 have been studied in detail, while the rest been used as validity references for relevant facts that surfaced during the research of this paper.

To this, two relevant cases from the author’s last employers has been used as indirect references. Due to non-disclosure agreements with the author’s last employer and the ITC customer to Case 4.2, exact details or text references had to be avoided.

3. Theoretical Framework

3.1 Perspective of information security improvements

As mentioned earlier in this paper and indicated by a number of sources (Chacos, 2014; (ISC)2, 2015; Fireeye, 2014; Riley, Pagliery, 2015; SANS,2009; OWASP, 2013; Badr, et.al., 2011; Malm 2015; Møllerhøj 2015; Satz 2015; Hart, 2015; Hansen, 2015) we currently see a paradigm shift regarding cyber-crime.

Still, the traditional internal threat stand for the primary incident volume. But from a financial perspective, external threats is becoming a substantially expanding economic risk factor (WEF, 2014; FBI, 2015). Something demanding that leadership realize this is not an IT issue, but a leadership issue demanding a place at the board table (Kotulica & Clark, 2003; Antilla et.al, 2004; Lindström, 2009; Soomro et.al., 2015). That the Information Security Officer need to belong outside the IT department, within Corporate Security (Harris, 2004; Bergsman, 2014; Coffman, 2014). The noted security consultant Shon Harris presented in a 2004 article, in an interesting comparison between how security adapted and non-adapted organizations behave regarding their strategies. Something the information security community should study in more detail (Harris, 2004).

Information Security has since the event of the first cyber-crimes, been regarded as a superficial topic. Like how it took quite some years before IBM implemented a true access management function with RACF in 1976. Before that their systems had been very rudimentary, regarding security features. And though most of today's Information Security systems are implemented with kernel APIs, most of them still behaves like backpacks to the system they protect.

We do see changes, like development of Microsoft Active Directory or Oracle Identity Management. However, we still have to see a such an elegant control process like AT&T Bell Labs Plan9's Factorum (Cox et.al., 2002). Though lying on top of the operating system, Factorum had a process and access control and granularity, not rivaled by any of today's systems.

But the main area of improvement should be to enforce use of security "best practices" like OWASP Top 10 and SANS Top 25 Vulnerability mitigations (OWASP, 2013, Christey, 2011), where we see vulnerabilities, known since the early 2000, still being exploited. We also have ISACA, CSA, NIST and ENISA Best Practices to guide us. But why not used? Maybe we have simply a too inexperienced coding workforce. We not only need to improve Information Security teachings, but how to code securely.

A challenge for our teaching establishments, as related a number of times by the noted security researcher, Gene Spafford, at Purdue University (Spafford, 1997/2000; Spafford, 2001; Spafford, 2009) before US Congress. Professor Spafford's conclusions should therefore, particular in the context of the accelerating number of events of Zero Day exploits, be reviewed as proven beyond doubt; our systems simply are too vulnerable (Magnusson, 2009).

If automotive and aerospace industries delivered products to similar standards and quality, they would soon lose their customer's trust. Having for the last 30 years frequently heared sales representatives agree to flaws, to in the next breath say; "but there is a fix in the next version", one looses faith. In 1987-89, as TIO for a pension found, the author waited for a critical Oracle patch to a fault killing our systems. It surfaced first late 1991 and situation is no better today, most software systems requiring at least quarterly downtime to apply patches. Not working very good with today’s 365, 24/7 operations.

As noted, we are in a critical need of more information security knowledgeable programmers and project managers, than available today. We do need to improve and extend existing teaching programs, by teaching already existing best practices and known mitigations. No ICT student should exit his or her university, without minimum a quarter of a year of Information Security studies that valid to their particular study direction.

We also need to be able to update and refresh personnel out in the field, with updated knowledge of Information Security methods and processes, improving the status out in the organizations. Some is currently done by sending employees to congresses and short courses.

For, as a former CS teacher, CIO, TIO and ISO, it is clear that we do need a paradigm shift, also within the higher education curricula. By allowing these personnel groups to go back part time, say over 3-6 months. For this topic do not render itself to short refresh activities, cannot be properly covered during one or two 2-4 day courses or conferences per year. There is definitely a need for a deeper knowledge investment, if to take on the new cyber criminals (Kotulica & Clark, 2004). Any technical solution, without improving general knowledge, will be short-lived. We need proactive operations management and better developers.

3.2 Dynamics of security oriented network architectures

The foundation idea of this paper was developed out from Case 4.1 below, where therein referred network fencing solution been used as proof of concept, implementing network layering, using ready accessible methodologies and thus improve resilience towards attacks. A thesis supported by Leischner & Tews (Leischner & Tews, 2007), Kindervag (Kindervag et.al., 2012) and Reichenberg & Wolfgang (Reichenberg & Wolfgang, 2014), but also including an idea about integrating a messaging hub to achieve better control of the involved data flows and thereby achieve a simplified approach how to secure critical network traffic.

In the case of Case 4.1, in 2009-11 appeared pronounced pressure of reviewing such remediations. After being object of a forced divestiture, the local organization still needed to continue to have data exchange with the former mother company. But the divestiture also forced us to look for replacing mother company legacy with new slimmer solutions, like external services. One such action was replacing our super computer access with renting such as a cloud service. A situation more common today.

To this we had additional issues. Since we intended to widen cooperation with some competitors to our previous owner, questions around intellectual property protection became an increasing pressing aspect. Something driving the thought of using a security improved integration platform. To simplify both communication protocols used, as well as communication pathways employed, building in network security resilience as a base principle. Based on the “deny all” principle.

This way we could maintain a governmental, legally driven car platform cooperation with the former owner, while developing new ones with new partners; data and server accesses separated after project data flows. Communication re-using a previous used fence idea, layering the internal network like an “onion”. Note that our “onion” networking in no way was related to Tor “onion” networking, though they shared some common traits. It was based on improvement of traditional backbone networking, similar to the Forrester Zero Trust initiative (Kindervag et.al., 2011; Kindervag, 2012), though sectioning the network within the existing legacy network framework. The idea was later developed as the “ISOOM” model [Figure 1] at a succeeding employer, discussed inside a small Swedish info sec group. But due to global market changes within that employer, it came never up on the table for commoditization.

However, unexpected support for the model was gained during a sales pitch discussion with the CISO of a large global Swedish manufacturing firm, with +10.000 employees and global operations. Growing by acquisitions, it meant that the ITC environment was a hardware/software zoo, currently not supporting any common “Best Practice” security methods, many systems handled locally.

During our discussion it became obvious that the ISOOM model had some advantages in their operating environment. Particular by adding the idea of messaging as a general method of data transportation. Locked into a heterogeneous environment, the best place to start, is where one can disconnect systems that blocks remediation. By driving the internal data exchange to use a messaging platform, this customer saw a possibility to easier identify involved data flows, allowing more effective scoping of replacements, as well as with IPsec to protect communication over their un-secure global network. Much needed at this customer.

Unfortunately, due to leadership decisions, we could not go forward with a pilot. The case is therefore to see as an academic exercise, not a proof of the concept.

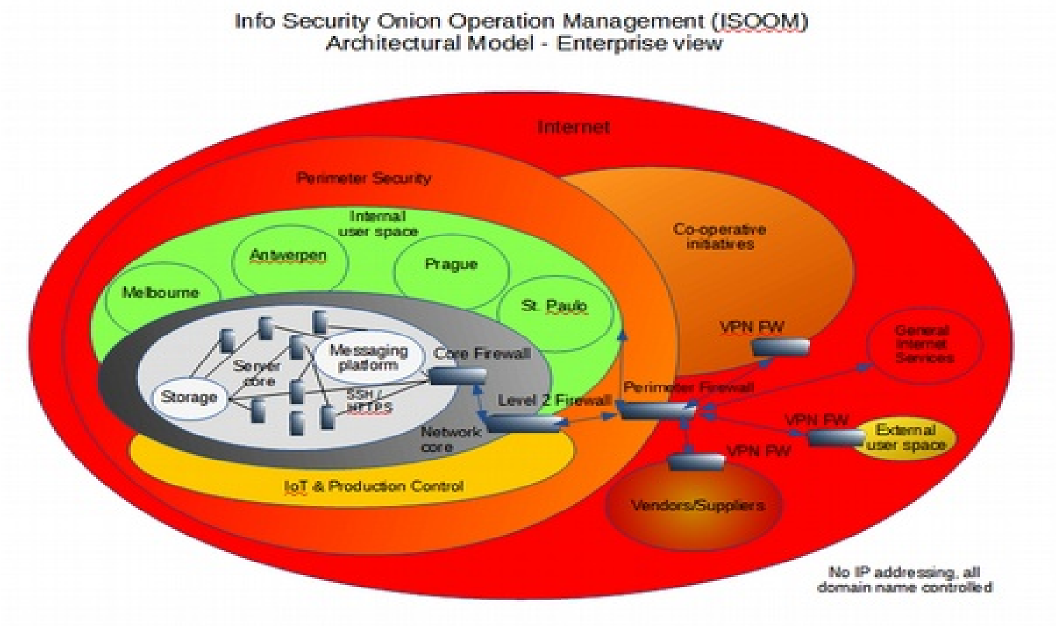


Figure 1: The ISOOM segregated network model

Having had insight in a number of other large organizations, neither Case 4.1 nor Case 4.2 is unique, there is globally an increasing need to make IT both securer as more flexible, to better fend of the risks that connections with customers, vendors and others constitute. As said in the beginning, most organizations save on operations, thus making themselves vulnerable. The ITC industry need to produce better architectural models, more resilient and flexible, than those used today. Not any easy operated solutions, demanding active managing (Reichenberg & Wolfgang, 2014).

SDN networks, an interesting candidate, is still lacking “on-the-fly” IPsec or other encryption, but we still have enough to implement something with what we have. Not to underestimate what we can do. We have AD and similar tools; we have VLAN technology. In itself not secure enough, but with IPsec a fully viable technology, securing both external as internal networks (Leischner & Tews, 2007). By analyzing core information systems’ communication, we can draw a communication map, enabling us to see what connections really exist and what protocols used, today using automatic mappers. It not only supports the security remediation, but improves the general network operations (Zimmerman, 2014). Remember, we cannot fully trust our CMDB, since it is largely feed by humans.

Based on this information we can divide the network into functional VLAN zones, defining protocols and connections that need to traverse between them, creating an “onion” network with core and perimeter firewalls. If traffic part of segments being connected over a WAN segment or having user segment VLAN traffic in parallel, we need to review if it is enough securing the VLAN traffic nodes (Rouiller, 2003; Leischner & Tews, 2007) or to add VPN protection. Administrative access and Storage networks (SAN/NAS), both reside on separate backbone networks, IPSec protected.

3.3 Integration as a security architecture tool

A key issue in most larger organizations or those having used IT for a long time, is the dependence of older, mostly vulnerable legacy systems. Far too many still rely on 1970: ies to early 1990: ies systems, currently making retired Cobol and mainframe programmers in increasing demand, no-one to replace them (Arstad Djurberg, 2016). With few, if any, educations addressing Cobol, Fortran, PL/1, flat or network databases or even C, those with legacy system managers need to be inventive when to maintain, patch or exchange their legacy.

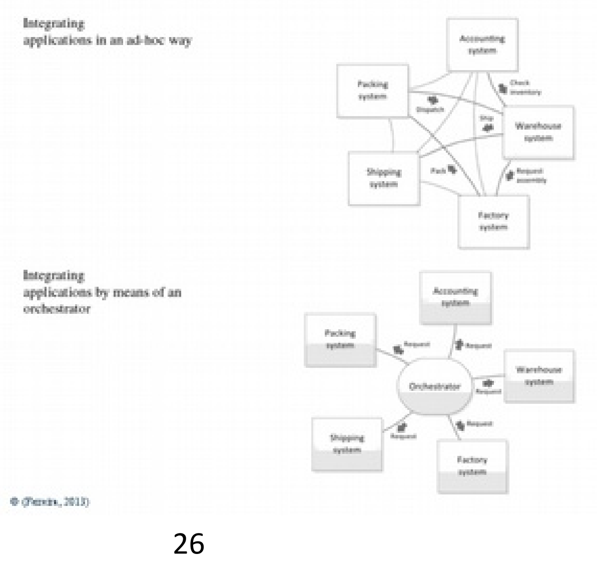
As said, we now need to build in protection and security measures in new ways, compare to traditional IT. But we still focusing on technology solutions that will fail us, as so many times before. It is time to look outside the box, to find mitigative methods that both protect better as supporting the ever ongoing migration out of the legacy. Unfortunately leadership tend to look at their ITC environment as a static feature, an investment to come an end, which it never do. Our ITC environments are dynamic, changing with business, independent if a private or public organization.

Therefore, our legacy systems has been unstructured adapted for the last decades; being rebuilt ad hoc, tweaked and having sub-standard additions to cope with the business changes (Talla & Valverde, 2011). Many, not unlike previous mentioned legacy communication, without proper change records or documentation. And with the responsibles having left. Many of these undocumented modifications being possible attack vectors for cyber criminals and internal opportunists. We also know from both praxis, as research, that “deny all, allow only business motivated access” will increase information security substantially (Fraser, 1997, Cheswick & Bellowin, 1994, Heidelberg, 2007(1)).

So how do we implement a “deny all” to these faulty systems, not stopping business. As earlier mentioned, this author suggests using a messaging hub solution [Figure 2]. Some systems will have complicated communications, including user access, media streams, SCADA/PLC connections or other multi-protocol methods. But most systems has basic data package or file transfers. This is particular valid in manufacturing, where “Just-in-Time” methods are used. A data package or a file transferred to be further processed. And not seldom we see same data going to more than one destination (Ferreira, 2013). In the 1990: ies and early 2000: s, many organizations tried to solve this with Data Marts. It is still today a viable, but costly solution, many going for the less costly messaging track. Products like WebSphere MQ, java based web services or even EDI.

Figure 2:

Ad hoc to hub migration.



© (Ferreira, 2013)

The key is that many of these platforms are multi-protocol in themselves, able to receive and send with sftp, smtp, EDI, web services and several data base connectors as Oracle SQL*Net and MS SQL Net. We can connect one system with sftp, another with web services and a third with a SQL connector. The involved systems do for most cases not need extra API: s and when access is established, the system connection can be protocol choked, to only the protocols required and to authorized sources, like the hub (Ferreira, 2013). Remember from 3.2, administration (and SAN/NAS storage) backbone is on a separate network interface.

To this, we can direct one input to several outputs. In some existing messaging platforms, data rewrites and processing is supported. The hub then able to adapt the data flow to the target's standard input API, without manipulating the feeding output. Result, better and simpler integration (Ferreira,2013). And as pointed out by Talla and Valverde in their paper, a more efficient remediation of legacy systems, is to perform gradual removal of separate sections of the legacy system (Talla & Valverde). Doing so with a modern messaging system, able to both remodel data structure as doing simpler calculations or processing, will allow us to migrate to more business adapted, modular system designs.

Naturally we need to review and map all active communications a system has, before re-mediating and implement hub communication, making appropriate changes to the counter art systems. But when attached to the hub, non-essential communication can be choked, performing a “block all” mitigation. Again, if not able to communicate, wide attacks, particular using vulnerable ports is no longer possible. If using IPSec or TLS, allowed protocols becomes securer, though TLS still have a risk of “Man-in-the-Middle” (Raza & Alli, 2013).

Still much overlooked, likely due to the exponential growth of system integration and falling behind of architecture during the last decade, making it hard to fend of business demands of testing different software, is Microsoft's Software Restriction Policy “deny all” settings in Active Directory. As concluded by Heidelberg (Heidelberg, 2007(2)), it will be challenging to implement in many organizations. We need to offer the organizations a middle ground, a general architecture, adopted to counter-act process and architectural limitations, allowing in one dimension and blocking in another.

All is not in place, a remaining issue, not addressed here, but needing mentioning. The increasing usage of ransomware, as good at encrypting non-file repositories, like traditional file repositories; as long as they can be reached by normal file commands. Which has been experienced with Sharepoint repositories.

This requires new ideas of protection against this type of attacks. Apparently the Anti-virus systems protect against them yet. And people still need write access to files, but can we protect against these devastating attacks.

3.4 Information security change process as strategic alignment

As said before, technology isn't enough, we need improved managed change processes. The critical key audit question, "Who did what and when and why". If no record, why a change was done, by who and ordered by whom, we cannot establish if an incident was malicious or just an accidental event. Our technical processes must be 100% review-able to establish both accountability, as allow for remediation of systematical issues (Magnusson, 2014).

One frequent reoccurring event, is software manufacturers sending out patches. Doing so, they often reset customers' elevated security settings back to factory default. After performed audits, each time this limitation was found in both operating systems, database systems as well as in business systems.

By using change records, it could be established that the contracted outsourcing vendor check the validity of new patches but never sent out remediation instructions to the server, database or applications admins. In simple context; "When this patch is installed, do check the configuration, since the patch resets them"-message never reached the operating teams. Remediation worked in the patch "test bench", but not applied in the "field", leaving critical security settings open after patches was installed. We need to catch those occurrences, so they do get distributed.

A more serious matter, ITIL do support management processes, but lacks some legally motivated processes for reach full hinterland support, to more efficient handle the critical management side of the change process, the approval process. By integrating administrative support processes better into our ITIL processes, we can decrease risk by system owners and administrators receiving a more current picture of coming tasks that can affect the system status. Tasks that sometime is readily identifiable as weaknesses and require deeper reviews (Magnusson, 2013(1); Magnusson, 2014). It is also important to study old audits, SOX as well as normal audits. They are a key source of finding systimatic weaknesses in processes.

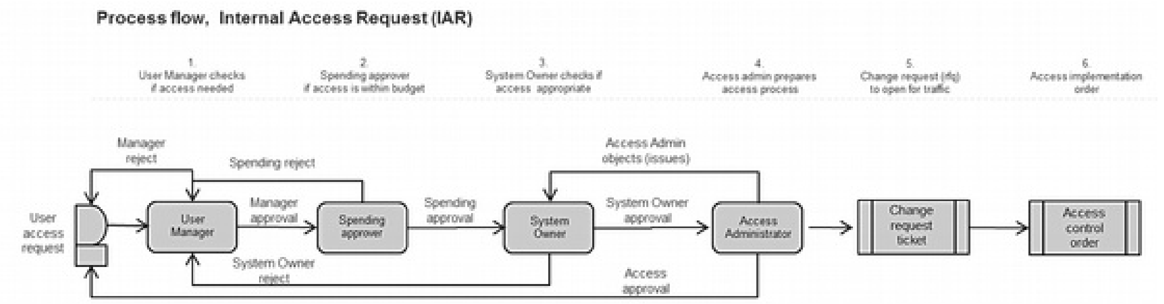
In several of in the media reported exploits, like Target, Goodwill, JP Morgan Chase, Home Depot, New York City and others (Hardekopf, 2015; Luckerson, 2014; Soomro, Shah & Ahmed,2016), un-authorized access to accounts was the main culprit, allowing the cyber-criminal to from these accounts seek elevated access to sub-systems and thus a possibility of injecting of malware. Simply a lack of administrative access logistics. With better access processes, likely most of them had been fended off before the perpetrators gained access.

Having taken part internal audits as ordering customer, manager or as delivering vendor project manager in 15 audits, also talking to several auditors about their audits, the most telling tale is the top six audit issues:

1. Incorrect access rights (access control)
2. No systematic responsibilities for accesses (access control)
3. Who did what, when and why (segregation of duty)
4. Lack of corrective actions and tracking (leadership/process)
5. Lack of documentation of decisions (leadership/process)
6. Failing code, patches or lack of "Best Practice" (leadership)

Items 1, 2 and to a part 3 has a common denominator, the users accessing the systems. Users like employees, consultants, external partner representatives or customer [representatives]. Here many have severe deficiencies in their tracking of user accesses, allowing for said exploits, not seldom using “dead” accounts, no longer used, but not removed (Magnusson, 2014).

Therefore, any information security remediation need to look at the present processes, find the flaws and proceed from there. One being to improve access approval control workflow prior to the actual ITIL change ticket flow [Figure 3], verifying the user as a valid user for access (HR involvement is implicit, HR personnel/consultant active lists being the needed data driver):


Process flow, Internal Access Request (IAR)
1. User Manager checks if access needed
2. Spending approver if access is within budget
3. System Owner checks if access appropriate
4. Access admin prepares access process
5. Change request (rfc) to open for traffic
6. Access implementation order
Manager reject
Spending reject
Access Admin objects (issues)
User access request
User Manager
Manager approval
Spending approver
Spending approval
System Owner
System Owner approval
Access Administrator
Change request ticket
Access control order
System Owner reject
Access approval

Note: User seek individual access; if a new employee, manager needs to proxy application requests, his/her manager to approve.. In many cases, but not all, user manager equals as spending approver, process cannot interpret such double roles. Access administrator notifies System Owner if any issues with change or respond to requestor, that order is approved and placed in the ITIL “request for change” (rfc) work order flow.

Figure 3: Administrative User Access Request process

This process needs to be reactivated for any personnel changes, as retiring, sick or parental leave, studies or changing department. Also, consultants which contracts terminated should be flagged and revisited by the user manager. In Case 4.1, this process was used since 1996, instigated by the then Process Manager. During the author’s time as owner of the processes from 2002 to 2009, when we were divested, we had only some singular audit remarks, some employees slipping due to HR not having accurate data. At the same time, colleagues around the world was plagued by having over 50% remarks, due to failing access control. As mentioned previously, HR must be included in the information security work (Magnusson, 2013(2)).

It also helps to have an Information Security Policy & Practices that could be followed within the intended ITC environment (Magnusson, 2011(1); Magnusson, 2011(2)). Writing a “must” document, not supported by realistic processes or having functional support is completely meaningless (Anttila et.al., 2004). Rather to step back and remediate processes to be more practically.

4. Cases

4.1 Case - Automotive

An automotive manufacturer, closed in 2011. Yearly production; 100.000 cars per year, 16.000 employees 1998, 5.000 at the closure, production volume the same. Sales global, with importers in over 35 countries and sales in 50, from Japan/Taiwan/Australia to US/Brazil. Owned daughters in Australia and 6 European countries, with Taiwan and Netherlands importers as free-hold, but over 80% IT integrated.

Up to 1990 being a part of a big Swedish automotive conglomerate, 50% was sold to a global US manufacturer in 1991. That later bought the whole company in 2000, again to sell it off to a Dutch owner 2010, to be declared bankrupt late 2011. During the period 1996 to spring 2011, the company was integrated into the US owner’s global network to 100%, with 90% IT separation achieved September 2011 by the divestiture project. The IT environment was declared a hardware zoo by the US CIO in 1999, consisting of Unisys, AS/400, OpenVMS, Solaris, IBM AIX, Linux and a number of generations of MS Windows, from NT to, in the end, Win2003. During 2000 to 2009 an integration project existed, broken off by the US mother company’s bankruptcy in late 2009.

Automotive industry and consequence of failing Information Security

Automotive is a very competitive and lean industry. Large scale use of IT goes back to the 1970: ies. Without IT, car factories die instantaneously. Something this author have firsthand experience of.

2008 my then US employer had a virus outbreak in an engine factory in southern Europe. As the European Information Security Officer [ISO], I was the point, clearing the infection out. Sitting 1000 km away, with travel restrictions. Due to reinfections and a faulty anti-virus tool, it took us a week to get it out, seriously hampering car production all over Europe, affecting some 20.000 employees. The leadership was not happy, we ending up challenging the anti-virus producer for damages.

All needed was a service technician from a company servicing test rigs, testing some engine parts before getting installed into the car engines. His USB stick with the program update for the test rigs was infected with a virus, our site clearance PC and the test rig PC’s/-controllers’ anti-virus program yet lacked a signature for. Not quite a zero-day exploit, but close enough. Result, a factory, normally building some 1.500 engines per day, standing still for a week. This was an information security nightmare no ISO wants.

This incident points to the critical effects we had to evaluate and understand during the case below. And why much of today’s information security processes is failing.

Integration as improvement - a long project

Let us start out with the intended case study, the now closed Swedish daughter company, a smaller manufacturing unit. While producing some 100.000 car per year, it was unique, it was a complete automotive unit, up till 2004 including its own engine and gear box factory. All in the same place.

Some background facts

The unit’s press shop had two large Hitachi presses, each with an individual installation value of $20-25M; the biggest 100 m long, 20 m wide and three stories high. Both with 4-5 built-in and non-exchangeable control computers, based on Windows NT.

All on the company network, no anti-virus available, since the anti-virus vendors stopped supporting NT years before, but needing to receive new production data and deliver statistics to other manufacturing systems. And you do not exchange some $25M manufacturing equipment, just because it's control computers was out of date. Not when having a financial depreciation time of 10-15 years.

To this, the unit's Unisys Mainframe programs was built in 1970: ies/early 1980: ies, most of them severely modified. As an example, during the spring of 2011, with limited manufacturing, we had an all-time high for CPU consumption. While manufacturing only ca 10.000 cars over 3 months, less than 37% of normal production. Primarily caused by less premeditated changes over 30 years. The other platforms, like AS/400, the Unixes and Linux was reasonably up to date, but 50% of the Windows control computers out in production was locked to a specific version of Windows, all automatic updating void.

Our tool vendors simply had used undocumented windows function and system calls to speed up communication with their tools, calls later removed by Microsoft, breaking any normal updating process.

This was the factual background, when this author was drafted as Technical IT Security Manager for the Swedish operations in 1999. Having looked at the issue already 1998, when as Internet Strategist having procured our first external Internet connection and firewall, I conferred with the local IT management about limiting the risks of our open network. We had external firewalls and protection of the WLAN nodes, passing our mother company's yearly audits, but inside was all open.

Due to the firewall service procurement 1998, the author succeeded to pass some base rules, as that no risk protocols were allowed through the firewall. Key was to block all not needed and use a basic firewall architecture that came from the Swedish military aerospace industry, improved with key functions for automotive supplier and dealer communication. Something becoming a continuous discussion with line managers, wanting to pass insecure IP protocols, as SMB and MS*SQL ports, over to suppliers. In total we were more than vulnerable if passing the perimeter.

Lesson learned – to be able to isolate at a crisis

When CodeRed hit about 2001 we had some hours advanced warning from a security service, we subscribed to. We got at 6 pm permission to stop all mail, even external, and other risk protocols to/from our mother company. In the morning, they and large parts of the world was standing still. By 10:00am we had new virus signature files and could open for email, both to the mother company and to Internet. FTP and some other protocols was still down another 24h, till all PCs' remediated. Our mother company was in a standstill for another two days, our primary IT vendor for four days, but we had full production, day and night shifts, during the whole incident.

This was repeated with SQL Slammer in 2003, but this time our mother company mimicked our 2001 action, blocking all out. All our vendors, again including our prime IT vendor, was completely out of business for several days, while we still were functioning.

The lesson learned; being able to isolate your operations is imperative.

When taking over as local ISO 2002, I tried to strengthen this rule. With some inspiration of the then appearing TOR network, it's onion model. The theory was, by fending of our central core systems, important manufacturing and development systems from system/resources outside our core, we would be less vulnerable from both internal users and external vendors/users. Traffic between each layer only to allow secure IP protocols, sometimes using a security proxy.

Separation in praxis

I must admit, it took to 2007 before we, with help of Sarbanes-Oxley [SOX] requirements, we could enforce any of this. SOX required companies listed on US stock exchange, to stop using insecure IP protocols, like ftp and telnet.

The Swedish unit had a critical system integration tool, called the "FTPShell", that with ftp as the transport layer dispatched some 60.000 messages per day between our 7 key platforms and ca 100 system. A poor man MQ Series, Seebeyond or JBoss. With some key show stoppers, our Unisys and OpenVMS. These didn't at this time have any alternatives to ftp. And sftp lacked some for us critical ftp functions we frequently used, "Append" and "EBCDIC" commands. The FTPS protocol had other serious limitations.

Solution was to a two-stage remediation. After discussions with the global SOX remediation managers, we agreed to do a subset of my onion model. Included SOX: ed servers was placed on a dedicated VLAN, allowing ftp between them, but fending of any ftp originating from outside or going out. A "ftp fence" was created.

The servers handling sftp could still communicate directly over the "fence" with that protocol, but no ftp. An access translation point, a multi-protocol server, understanding both ftp and sftp, previously used for Internet based B2B traffic since 2005, was integrated into the ftp fence, allowing a transfers between the FTPShell on the inside of the fence and sftp outside. The project took 7 months to prepare, identify and remediate fence traversing ftp traffic. Much due to some traffic being quarterly, only seen at the roll-over.

Not a perfect project, the night the fence was made active we registered nearly 1000 non-authorized connections. After the responsible Business Process Information Officer (PIO) reviewed these 1000 attempts, most was easily remediated. But some 200 attempts proved to be orphans. Some of them high volume orphans no-one missed and without change documentation. If placed in production or engineering, needing to get a file from any of the enclosed servers, one had to use a server, supporting sftp. The "FTPshell" still lived its life inside the fence, but very few could see this traffic. Everyone, except administrators, was denied access to the local ftp clients one the "FTPshell" servers.

This was later repeated with telnet, migrating to ssh, when Unisys released their ssh server around 2008.

The "onion" separation model - stage 1

When our US owner went into Chapter 11 2009, later declared defaulted by US government, we were put up for sale. After some negotiations, it ended with us mid-2010 being bought by a Dutch company. This had some radical influx into our new ITC strategy, developed the winter/spring of 2010. For Information Security, there was a couple of new elements to handle;

- We were still to have some co-operation with the successor to our US mother, driven by legal car certification processes in a large number of countries. When they changed a so called platform that we still used, we needed to acquire those changes and vice versa.

- We also had one of our models built in one of their Mexican factories. Exchange of advanced CAD models, part lists and ordering information had to flow freely.
- Our new owner intended us to offer engineering capacity to previous non-affiliated automotive manufacturers, requiring information insulation toward our previous owner.
- We also looked at doing special work for industries outside automotive, like aerospace. An industry area very similar to automotive, but with very high demands regarding information security.
- And, lastly, we needed to slim our organization further, we no longer had responsibility of developing whole modules for a company manufacturing around 8 million cars per year, just for 100.000 per year. So we got a lot of IT overhead, not needed.

Key was to scale down everything, including ITC. Try to get out our Unisys, moving Solaris and AIX to Linux, standardize Windows to one client release and servers/controllers to Win2008 and to better secure any old "crap", not interchangeable. In the long run the AS400 was to go Linux as well. Supercomputer capacity was leased as a semi-cloud/- semi-outsource service.

But how to do this?

Together with the network manager and the local SOX transition manager, the author dusted of the old "onion" model. To with VLAN networking build sectioned virtual IP network shell around the different identified server units. Also, after in September 2011 becoming the company's last Enterprise IT Architect, I started a discussion with several system owners, about using the messaging system as a pro-active system remediation.

And by stopping any direct communication between non-time critical systems, letting them store data centrally in a data switch like MQ or Seebeyond, like a simplified data mart, re-sending data to approved receivers. It would allow us to easier change and remove redundant systems. For example, demount sections of the Unisys, move remaining internal API: s to the switch and process data in a new, resized modern solution. However, our bankruptcy came to early.

The system management angle

What we learned by the ftp-fence 2007, was that some 25% of all non-FTPshell ftp connections was dead transactions. Either the sending part never sent any usable data or the receiving system never processed it. Because no-one closed down their redundant communication. One reason was lack of API change documentation, no-one knew why a particular transfer existed, who ordered it or what it supported. So no-one dared to close it down. A clear Information Security risk, an attack vector into our systems. The information should have been in our CMDB, but most of these connections seemed to have been created as emergency solutions, no change documentation done, simply created ad hoc between the system owners and our primary IT vendor.

Before trying to do a project like our ftp fencing, one therefore have to do a network analysis and identify seen traffic, taking 3-4 months. With some traffic being only at quarterly roll-over; the first quarterly pass after putting up the fence, we caught some 20 new ftp connections. Our intention was to replace existing traffic with sectioned VLAN/IPsec based connections from the line environments, tunneled through an internal choke firewall to a messaging system, allowing only needed messaging protocols, all others blocked.

That way we intended to reduce the risk of using zero day or known exploits. Each line's production equipment only to see it's the designated messaging connector; acknowledging only pre-defined line hosts, effectively blocking all non-authorized traffic. Even if not going to the extreme of the Forrester Zero Trust networking (Kindervag et.al., 2011) IPsec had insured that Man-in-the-Middle attacks would be harder to perform.

Having a sectioned network architecture, with production and core IT secured this way, using messaging, would have vastly improve security of operations. Allowing it to easier exchange unsecure older or redundant components with more modern solutions, modularity becoming the founding principle of the overall architecture (Bossert, Richter & Weinberg, 2015). A lot of this has been seen in the integration of data flows with standard Unix Tools. By exchanging involved tools in the data flow, data can be manipulated by Unix Tools in ways only rivaled by Perl and maybe Python (Kernighan & Plauger, 1976; Seebach, 2009; Tailor, 2004). A functionality model, possible to implement with messaging.

Future Mode of Operations - never implemented

Our intention was by this way build a secure central network shell around the core systems and at the same time give systems owners a possibility of analyzing incoming and outgoing data, creating a better vantage point over what data flows to keep and which to change. Allowing more flexible data connection, needing less rebuilding of the applications. When business and processes changes; exchange processing modules.

In November 2011 we had a basic template to a more resilient IT structure, with stringent and much easier managed control of data flows, not allowing un-authorized network traffic, but due to the financial status and later bankruptcy, reality never went beyond the ftp- and telnet fence.

Conclusion

As a small independent automotive manufacturer, intending to cooperate with a range of partners, that was something that being trademark for the brand since the early 1980: ies. But new interactions required better protection of both own intellectual property and capital, as at the same time not creating liabilities, exposing others property we processed. All demanding better secured information systems and data flows.

At the same time, slimming of the IT environment was paramount. A small 100.000 car manufacturer could not sustain an IT environment built to work in conjunction to other global manufacturing processes for millions of cars, not even the 250.000 the local assembly line was design for. Having primarily legacy systems, adopted to fit in a modern order driven "Just-in-Time" process, much had become a trade-off between cost depreciation, financial plans, functionality, time and how to solve acute integrations.

Unraveling all this to a modern scalable and Business Process adaptable architecture demanded the need for simple plug in and out modules, without noticeable downtimes. A perfect case for a "onion" based network and messaging as a core function, isolating direct accesses. The natural evolution, since we did have 30 years' operational experience using the FTPShell messaging system. With an improved change and documentation process all bought into.

4.2 Case - Manufacturing

A global Swedish technical equipment manufacturer, with presence in +50 countries and manufacturing units in more than 70% of these countries. With a large cadre of international employees, it has grown primarily by procuring competitors.

As a consequence, like our previous case, it is a hardware "zoo", anything from IBM mainframes over AS400, OpenVMS and Unixes to Linux, Windows and production/test equipment. The main ITC offices is in Sweden, but due to time criticality, a lot is install out at location. Since most of this came with the procurement of the previous competitor, in principle, each manufacturing country has its disparate flavor of software, hardware and network standards. All linked by a high capacity global gigabit network, down to all regular offices. No internal firewalls, one open network, no IDS/IDP, neither on network nor servers. All servers visible for anyone on the network.

Philosophy of Manufacturing IT

A key issue within manufacturing is, "if it works, don't change it". Even minute IT changes can stop a manufacturing unit, as the lesson learned in last case.

Why?

Not seldom, the driving force of manufacturing changes are the local maintenance crew, documenting changes after production standards, not IT standards. Often these crews are shop floor engineers, having learned IT, not IT technicians. Which is logical, since they handle production equipment with IT, not IT systems with production equipment. This is not the world of IBM, HP, Dell, Oracle, SAP or Accenture, but the world of ABB, Siemens, Dürr and a few other companies, producing PLC/SCADA and test rig systems. Close to not even being on the same planet.

Therefor the local site managers have the upper hand toward the IT organization, regarding how to handle replacements, upgrades and, not the least, information security. Known is secure, new stuff might need a complete and working test line to check out the new equipment, before introducing it. Test lines that is expensive and take time for an already understaffed maintenance crew. In that context IT people is just an ignorant nuisance.

Local manufacturing network can be 15-20 years old, even running on coax and old Token Ring routers. Or being of Cat3 network standard. With incomplete network maps over where outlets are. How do you secure such an operation, without unacceptable costs? This company had one particular notorious IT outlet; an open network outlet in the public stairwell of the office house they rented offices in. And the local manager could not understand why corporate security wanted to disconnect it. That anyone could attach a laptop and see the complete global network was not a motivation.

Attitudes towards Information Security

Another issue was that several of the subsidiaries still behaved as if being totally independent of the mother company, thus driving their own IT strategy, completely dissonant to the central strategy. Meaning own network solutions, Internet access, server and PLC/SCADA solutions, HR systems etc. The company had a total of ca 50 Internet connections spread over the world. To enforce Information Security in such a decoupled firewall environment is short of haphazard.

The author related in the discussions with the Case 4.2 CISO, of the experience, my old US mother company, 10 times bigger than this Swedish company; we also had 50 local firewalls. But all these was under central change control, nothing changed without our Red Team done a review or CISO given his approval. When on a global network, thinking we can manage our own local firewall independent, that is to gravely misunderstand our responsibilities, making us liable for legal actions, due to any cyber-crimes using this local firewall.

Here the author referred back to Case 4.1, where we already 1999 removed all local firewalls at our sales offices, including our non-owned Taiwanese and Dutch importers, replacing them with a IPsec "black" box VPN over Internet. With general 2Mb Internet connections, 6 European countries, Australia and our two external importers, all their Internet connections passed over the Swedish core firewall, including time critical dedicated VPNs to national DMVs for those having such, like Australia.

None of the sales offices saw any negative consequences by not having local firewall, rather they felt tighter integrated into the Swedish main office. Referring this to the CISO for Case 4.2, the immediate response was that it looked like what he wanted; but unfortunately a scenario not to be supported by neither regional nor local managers.

Possible steps of remediation and mitigations

Further, in the author's discussions with the CISO, we reviewed a number of other possible solutions to the inherent liabilities. One was using IPsec encrypted VLAN technology, building a separate protected core VLAN network, with an internal firewall "fence", then other VLANs for regional key servers, independent where placed in a single region. This to minimize change risks, with only core routers involved and all VLAN traffic behind the routers encrypted via router to router IPsec encryption.

Advantage would be that, though located at many places, the core and key servers would have a basic router based firewall protection, only allowing business motivated protocols to pass and to enforce centralized administration processes. PLC/SCADA and other time critical equipment would still be on local production VLANs', separated from both the core/key servers as well as from user space. As with the core, these VLANs' also would be protected, initially with router filtering, again allowing only approved protocols.

When enforced, the changes could be integrated in stages and issues as access control and change processes could easily be streamlined, in the end allowing for one unified process. We need to remember, the key issue in these environments is that the maintenance crews never use normal access control processes. They take too much time and the benefit of them is on the floor personnel is regarded as non-existent. That is, until disaster strikes.

During the author's 30 years in the business, IT historically have been unsympathetic to the floor or maintenance crews' situation, not speaking their language. These cannot wait 24-48 hours for a password change or other corrections, if a line is stopped, it is paramount to get it back in order within the hour. Anything stopping production is bad for business.

We therefore need better processes that support these work tasks. Something coming to slowly, like self-password reset or simple onetime passwords. We also need to have solutions that support physically dirty and not always EMF clean production environments, as well as providing for 5-10 people in line teams, all using the same line terminal. In many cases, that means no password or all using the same. In the end, requiring mitigative and compensatory actions. However, such was not discussed in this case, just how to unify the password process and create the, in the previous case, mentioned "onion" solution. Due to unrelated reasons, the author leaving the sales case for other duties, our discussions ended there.

Conclusion

With such a heterogeneous environment as in Case 4.2, all levels of Information Security will eventually fail, since no overall control, particular access control, is possible. Likely the company had a number of non-authorized individuals and groups on their network, due to lacking any form for network surveillance, as well being an interesting target for industry espionage.

Simply, the leadership team only saw to the budget bottom line, not the risks and liabilities they faced. Question is if they even understood what risks and liabilities they faced. If being a shareholder with knowledge of the situation, this author would have questioned the competence of the leadership team.

A stock exchange trader would likely negatively balance the risk perspective, when evaluating the trading positions. Likely much in the same way, as VW saw their value reduced with up to 20%, after been found out that they faked their diesel emissions (Kresge & Weiss, 2015).

Leadership teams need to take cyber-crime as serious as traditional industrial espionage, since that is the new way of doing such activities. Again, this is not a CIO question, due to the legal implications, it is a leadership issue (Antilla et.al.,2004; Kotulica & Clark, 2004; Lindström, 2009; Soomro et.al., 2016).

5. Analysis

Due to not having any current empirical experience or any concurrent cases to relate to, some of the base for an unequivocal conclusion is sadly lacking. However, combining work experience of architecting operative solutions for 9 employers over 30 years, extrapolating the two presented cases and reviewing a number of related papers, some relevance for presented views of the topic area should be present. Several of reviewed papers did themselves extracted their conclusions based on mainly literature studies and at mostly 1-2 test cases.

By extrapolating the cases at hand and the articles, supported with experienced "do" and "don't", we see a vastly fractional ITC landscape; business area managers more frequently driving changes, the ITC department no longer is scoped to handle. Business then buys external, often cloud, services not easily integrated into the existing landscape, as well as departments respectively investing in overlapping and non-compatible ITC solutions, to later finding their data flows clashing.

The consequence of this fractional evolution is a legacy that lacks control and proper security measures, leaving holes in the protective layer. Want again point to Stafford, Kindervag and Bossert (Stafford, 2009; Kindervag, 2012; Bossert et. al., 2015), all explicitly pointing this out. We need to change, to improve our systems resilience to ever-increasing smarter cyber-attacks. Resilience supported by better management processes and multi-level protection architecture.

Perimeter protection, network layering, encrypted connections, simplified communication paths, modularized, exchangeable systems, better change control and putting responsibility where it is due, to make internal "offenders" accountable. And doing so out of a data flow perspective, understanding why a data set need to be at a given place at a **given** time, who decided so and what liabilities the chose solution will impose on the organization. To this, we need to find ways to implement such a program, without disrupting day-to-day operations.

ITC need to be better at understanding how other departments functions. At the other side, due to improved processes, other departments, particular HR need to understand their ultimate role as data maintainers and source of needed personnel information to implement the expected future security framework.

We also need to question if our current IT platforms really can evolve to become securer. A band-aided solution, where more Band-Aid is applied, where is the trust. We need to challenge Microsoft, the Linux and BSD communities, IT establishment etc., if their platforms haven't reached "End of Life" already. We probably need simpler platforms, more like AT&T's 1990 Plan9 operating system, with its more resilient security system, Factorum (Cox et.al., 2002). Though Plan9 and Factorum is dead, they represent a sounder starting point than Linux and Windows. Plan9, Factorum and virtual, but secure, Docker instances as sandboxes. And that the hardware manufacturers are disallowed to merger failing drivers into the OS kernels. With today's technology, this is a redundant methodology, clean APIs'.

And to conclude the analysis, the leadership must actively involve themselves to market the need of a modern Information Security Policy & Practice and its impact on each employee, that it not a showcase but matter. Without the legitimacy of the leadership, all change will fail.

6. Discussion

We need more research, how to do all this, finding sound development models helping hardware and software creators to make risk free solutions, as well as help management responsible to dare to go for needed resilient solutions. How to, by using network sectioning and fencing together with secure gateways, proxies and other protective measures, survive and migrate into a less risk prone ITC environment.

Most has already been mentioned, strengthen policy and processes, but so they are seen as realistic, block not needed network traffic, simplify network flows and support system replacements by using integration tools like messaging systems. Doing so, without disrupting business, by better understanding the business side's limitations and boundaries.

As noted in the previous section, the leadership need to understand their responsibilities, regarding the organization's data, including legal liabilities. Information Security has to be sponsored from the top, as seen in several articles (Antilla et.al.,2004; Kotulica & Clark, 2004; Lindström, 2009; Soomro et.al., 2016). When delegated to the ITC department, the rest of the organization will see Information Security policies and practices as a pure ITC affair, nothing the rest of the organization need to bother about. Due to this, during the last couple of year, a discussion regarding the need of moving Information Security out of the ITC department, to the CFO or COO offices has intensified (Harris, 2006; Bergman, 2014; Coffman, 2014; Liv, 2015).

Still, without the CEO stamp of approval, Information Security will continue to live a hap-hazardous life, the organization continuously being unnecessarily exposed. As this paper tries to establish, a perimeter control is not enough, we need the whole context to work, from the process side to implementing out-of-the-box solutions, disrupting the anticipated architecture and processes. Doing the unexpected in the right way, will help to raise the protective fence higher. The tollgates can be as follows:

1. A general improvement plan, based more on changed processes and more realistic policies and practices. Any change is done with existing resources, as far as possible.
2. Selling in the plan, not only to the CIO, but to the leadership team, acquiring a team sponsor. Without a formal sponsor, the plan will die.
3. Learn to understand the data flows, not only locally, but from/to governmental agencies, dealers, suppliers, ITC vendors and partners.

   Offer a university to do some master thesis, getting an outsiders view. Requires mentor time and outsider access, but after writing my own master thesis for an oil company, all data confidential, it can be arranged satisfactory.
4. Knowing the data flows, it is time to review protocols used. Which and how to limit them. Fencing or encrypted network or a mix. Where to place internal firewalls or choke points. What servers need to be accessible by people and then via what protocols.
5. Make a criticality list, what to do first, how and when. Continue down-wards, creating a more detailed project remediation plan.
6. As said, no technical plan is complete without the process support. See over the change processes, that the ordering party is involved to understand that quick fixes will make them liable for any consequences. It takes time, but they will come around, believe me.
7. Kick HR's butt. Yes, you read right, kick their butt. As mentioned in 3.4, incorrect accesses stand for an unequaled majority of all cyber-crimes. We need to become far

better to handle these. An Excel spreadsheet, updated two years ago will no longer do. Accesses is change items, always documented in the change systems.

As mentioned in the process section, HR's role is to alert when a person changes position, leaves or has their employment changed in anyway. Even for consultants and other externals we allow in. HR are the place where this data is best handled.

8. Review messaging options, chose a hub tool mapping the organization's foreseeable future. Trim it in, develop standard change processes for exchanging direct systems connections into the hub. Ready templates, independent of IP protocol used.
9. Get the project going, remediate after plan. It will take time, but the more confident business and ITC gets, the quicker the remediation will proceed.
10. Check that allocated server groups is indeed protected from unauthorized communication and thereby from attacks. Now it is time.

A big project, yes, but if reducing risk, we do improve our surrounding's trust, something also improving eventual stock market evaluations. If we can build resilient space crafts, bridges, airplanes, cars and boats, why not IT environments.

7. Conclusion

The author like to repeat a citation from Prof. Gene Spafford, tribute to both Albert Einstein and the 1600 hundreds British writer John Dryden: “Insanity: doing the same thing over and over again expecting different results”.

Yes, we humans do this a lot, independent how intelligent we are. The British military psychologist Norman Dixon describes this very elegantly in his 1976 book, “On the Psychology of Military Incompetence” (Dixon, 1976). Dixon reviews a number of British military campaign leaders from Krim to WWII, the failures they develop with, may I say, a certain elegance, but at horrible costs. Due to personal preconceptions, though the signs of the opposite was clearly seen, they made catastrophic mistakes.

What Dixon describes can be seen in any organization and very often when discussing ITC changes, repeating the same thing, expecting a new outcome. We dare seldom to change, what we know is comforting, even if we sail toward that iceberg, like Titanic did. The maxim “do not change what works”. Well, it might still work, but what is our liability due to it. Having the front door open works fine, but for everyone. Also those with criminal intent. While our insurance policy requires us to consciously behave so that we reduce the ability of these elements to exploit our weaknesses, with consequences. If we keep the door open, the policy is rendered invalid.

We have to realize that, independent of organization, even NSA as Snowden proved. We have these human limitations and liabilities and have to act accordingly to counteract them. We see a change in how cyber-crime evolves. Developing faster and more aggressive than our ability to defend ourselves. Where best defense is thinking out of the box, starting with “Deny all, allow what’s needed”.

It is a sound principle, as proven by several papers and security policies (Fraser,1997; Heidelberg, 2007; OWASP, 2013). If done with afterthought, the Information Security function does not need to say “No”, but can actively help business to find as good solutions that satisfy both business demands as well as the security requirements. But here business need to approach the Information Security function in good time, not as an afterthought, “Oh, we also must …”.

Information Security must be proactive, learn enterprise and system architecture, as well as motivate other groups to understand the data flows and how their solutions affect security. Doing so, we can build defense architectures that gives the “bad guys” a “chewiness” that hopefully drives them to concentrate on easier targets. We are not talking any radical evolution to solve this, we simply need, as discussed in this paper, to use the tools already at hand. But, still remember, there is nothing as a “secure system”, only “a bit securer system”.

In the end, we still need to reflect over the quality of software, independent if applications, system or network. No consumer would accept to change or “update” a car, a stereo, a refrigerator or duster, in the same way as the software industry forces their customers, due to hap-hazardous development methods. After sitting three years in the middle of a coding factory, I often related to Fredrick Brooks experiences from leading one of IBM’s coding teams for OS/360, visa-vi the other teams. As related in the book the Mythical Man Month (Brook, 1982) and made valid from the author’s experience as TIO in the late 1980: ies, delivering support to two application teams, one traditional and one unwittingly organized after Brooks template.

Not only was the smaller “MMM” team three times faster for an equally large system, it had fewer software errors, integrated changes more efficient and the application worked as expected when put in production, on schedule. The other team had to through all out and start from scratch 1.5 year later.

We need to improve this, we need to, as Prof Gene Spafford said at a US Congress hearing in 2009, make the software producers to be accountable and liable for consequences of their sub-standard products (Spafford, 2009). But, as Spafford also said and the author has experienced at the coding factory I sat in, we need to produce personnel that is far more knowledgeable of the topic. Already before a CS student begin to drill down in his/her subject, they need to get a thorough and mandatory introduction to Information Security. In their basis year to become exposed to “Best Practices”, OWASP Top 10 and SANS Top 25.

Students going the process route need to be exposed to consequences and liabilities, to create best practices and checklist that works, to talk with Information Security people from outside the academic world, standing in the “trenches”. Programming and network students need to drill down in the vulnerability mitigation lists, “how to”, knowing them by heart. This information exists since long, but after talking Information Security to fresh CS students coming into my different employers for a couple of decades, apart from a few, they all looked like question-marks.

Not only more Information Security students is needed, but more security savvy students in general. They need to understand this, before they drop out, being headhunted by a firm in dire need of new cheap coders. To this, a good CS employee has to be a “Renaissances Man/Woman”, something to seldom met out in the “wild”. Having a broad understanding of IT / ITC decreases the risk of insulating the mind, being “nearsighted”. As far too many of the several hundred programmers and consultants this author met over the years have been.

Information security needs a far better foundation, and that foundation is the people designing and developing our IT systems. Not to remediate and mitigate the current state, that just a necessary Band-Aid to survive till we learn how to build right.

8. References

Books:

Brook, F.P., 1982, "The Mythical Man-Month: Essays on Software Engineering", Addison-Wesley, Boston, MA, US

Cheswick, W.R., Bellowin, S.M., 1994, “Firewall and Internet Security”, Addison-Wesley, Reading, MA, US

Dixon, N.F., 1976, “On the Psychology of Military Incompetence”. Jonathan Cape, London

Ed., 2008, “Data Breaches Trends, costs and best practices”, IT Governance Publishing, Ely, UK

Ferreira, D.R., 2013, "Enterprise Systems Integration: A Process-Oriented Approach", Springer Science & Business Media, Berlin, DE.

Ford, H., Crowther, S., 1922, “My Life and Work”, Garden City Publishing Company, New Your, US.

Garfinkel, S., Spafford, W., 1996, “Practical Unix and Internet Security”, O’Reilly, Sebastopol, CA, US

Hayden, L., 2010, “IT Security Metrics: A Practical Framework for Measuring Security and Protecting Data”, McGraw-Hill, NY, US

Kernighan, B.W., Plauger, P.J., 1976, “Software Tools”, Addison-Wesley, Reading, MA, US

Palomar, E., Suarez de Tangil, G., 2013, “Advances in Security Information Management: Perceptions and Outcomes, In Computer Science, Technology and Applications”. Hauppauge, New York: Nova Science Publishers, Inc.

Seebach, P., 2007, “Beginning Portable Shell Scripting”, Apress, Berkley, CA, US

Taylor, D., 2004, “Wicked Cool Shell Scripts”, No Starch Press, San Francisco, CA, US

Velte, A.T., Velte, T.J. & Elsenpeter, R., 2010, “Cloud Computing, a Practical Approach”, McGraw-Hill, NY, US

Wurman, R.S., 1997, "Information Architects", Graphis Inc, New York, NY, US

Reports:

Abad-Carrascosa, A., Marin-Lopez, R., Lopez-Millan, G., 2015,"Software-Defined Networking (SDN)-based IPsec Flow Protection", draft-abad-sdnrg-sdn-ipsec-flow-protection-00, Internet-Draft, IETF, July 19, 2015

Federal Bureau of Investigation, “Internet Crime Complaint Center (FBI)”, 2015, 2014 Internet Crime Report, FBI, Washington, US

Fraser, B. (Ed.), 1997, "Site Security Handbook", IETF rfc2196, IETF 1997.

Joshi, R., 2007, “Data-Oriented Architecture: A Loosely-Coupled Real-Time SOA”, Real-Time Innovations, Inc., Santa Clara, CA, US

Kindervag, J., Wang, C., Balaouras, S., Coit, L., 2011, “Applying Zero Trust To The Extended Enterprise”, Forrester Research, Camebridge, MA, US.

Kindervag, J., 2012, “Build Security Into Your Network’s DNA: The Zero Trust Network Architecture”, Forrester Research, Camebridge, MA, US.

Leischner, G., Tews, C., 2007, "Security Through VLAN Segmentation: Isolating and Securing Critical Assets Without Loss of Usability", 9th Annual Western Power Delivery Automation Conference, April 3–5, 2007, Spokane, WA, US

Lindström, J., Magnusson, L., Sporrong, P., Berglund, U., et. al., 2015, "En praktisk och lite enklare checklista för införskaffande, användning och lämnande av molntjänster", CSA Sweden, CSA, SE

Magnusson, L., 2009, "A Security Practitioner's view on Internet Protocol"s, IETF Internet-Drafts, draft-magnusson-secure-practice-00, IETF.org

Magnusson, L., Salomé, S., 2012, "20121112 - Sollentuna Municipal Cloud Best Practice Checklist v1.5D", Classified Report, Sollentuna Municipal IT Board, Tieto Sweden.

Raza, H., Alli, Z., 2013, "Investigation of Solutions for Intrusion Prevention and Detection", Master thesis, School of Information Science, Computer and Electrical Engineering, Halmstad University

Rouiller, S.A., 2003, "Virtual LAN Security: weaknesses and countermeasures", SANS Institute, June 19, 2003.

Spafford, E.H., 1997, "One View of A Critical National Need: Support for Information Security Education and Research", COAST Project and Laboratory", 105th Congress, US Senate Committee on Commerce, Science and Transportation, revised July 17, 2000.

Spafford, E.H., 2001, "Cyber Security — How Can We Protect American Computer Networks From Attack", 107th Congress, US Senate Committee on Commerce, Science and Transportation, Oct 10, 2001.

Spafford, E.H., 2009, "Cyber Security: Assessing Our Vulnerability and Developing an Effective Defence", 111th Congress, US Senate Committee on Commerce, Science and Transportation, Mar 19, 2009.

Stevens, J.F., 2005, "Information Asset Profiling", Carnegie-Mellon (www.sei.cmu.edu/publications - CMU/SEI-2005-TN-021), Detroit, US

Tashi, I., Ghernaouti-Hélie, S., 2007, "Security metrics to improve information security management", Proceedings of the 6th Annual Security Conference, April 11-12, 2007, Las Vegas, NV, US

World Economic Forum/McKinsey & Company (WEF), Jan 2014, "Risk and Responsibility in a Hyperconnected World", Geneva, CH

Zimmerman, C., 2014, "Ten Strategies of a World-Class Cybersecurity Operations Center", The MITRE Corporation, Bedford, MA, US

Articles:

Abraham, S., Chengalur-Smith I., 2010, "An overview of social engineering malware: Trends, tactics, and implications", Technology in Society Volume 32, Issue 3, August 2010, p183–196, London, UK.

Anttila, J., Kajava, J., Varonen, R., 2004, "Balanced Integration of Information Security into Business Management", IEEE, Proceedings of the 30th EUROMICRO Conference (EUROMICRO'04), p558-564

Badr, Y., Biennier, F., Tata, S, July 2011, “The Integration of Corporate Security Strategies in Collaborative Business Processes”, IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 4, NO. 3, p243-254

Bandyopadhyay, T., Jacob, V., Raghunathan, S., 2010, "Information security in networked supply chains: impact of network vulnerability and supply chain integration on incentives to invest", Info Technological Mag (2010), Springer, March 2010, Vol 11, p. 7–23

Behl, A., Behl, K., Behl, N., 2012, "Multi-Tiered Architecture for Intrusion Prevention", Journal of Information Technology Infrastructure, Vo1 No2, Nov–Dec 2012, p19-22

Böhm, M., Fähling, J., Yetton, Ph., Nominacher, B., Leimeister, J.M., Krcmar, H., 2010, "IT CHALLENGES IN M&A TRANSACTIONS – THE IT CARVE-OUT VIEW ON DIVESTMENTS", International Conference on Information Systems, ICIS-0363-2010.R1, Feb 8, 2012

Donaghu, M.T., Barff R., 1990, "Nike just did it: International Subcontracting and Flexibility in Athletic Footwear Production”; Regional Studies; Vol. 24, Iss. 6

James, H.L., 1996, "Managing information systems security: a soft approach". IEEE, In Information Systems Conference of New Zealand, 1996. Proceedings, p10-20

Jonker, M., Sperotto, A., 2015, "Mitigating DDoS Attacks using OpenFlow-based Software Defined Networking", Intelligent Mechanisms for Network Configuration and Security, Lecture Notes in Computer Science, Springer International, Vol 9122, p 129-133

Kotulica, A.G., Clark, J.G., 2004, “Why there aren’t more information security research studies”, Information & Management 41, Springer Verlag, p597–607

Lim, S., Ha, J., Kim, H., Kim, Y., Yang, S., 2014, "A SDN-oriented DDoS blocking scheme for botnet-based attacks", 2014 Sixth International Conf on Ubiquitous and Future Networks (ICUFN), 2014, July 8-11, p63-68

Magnusson, L., 2011(1), “Global Insight: A Call for Best Practice Framework”, Information Security Professional, Issue 14, p32(ISC)^2, Farmingham, MA, US

Magnusson, L., 2013(2), “Global Insight: HR Access-Key to better InfoSec”, Information Security Professional, Issue 22, (ISC)^2, Farmingham, MA, US

Magnusson, L., 2013(1), “Informationssäkerhet på 2010-talet”, Chapter 12.3, IT-management, as “Magnusson, K.”, Bonniers Ledarskapshandböcker, Stockholm, SE

Magnusson, L., 2014, “Auktorisering-accesskontroll som nyckel till bättre IT-säkerhet”, Chapter 12.6, as “Magnusson, K.”, IT-management, Bonniers Ledarskapshandböcker, Stockholm, SE

Mayrl, Ch., Tröscher, F., Abeck, S., 2006, “Process-Oriented Integration of Applications for a Service-Oriented IT Management; Integrated IT Management Architecture”, Business-Driven IT Management, April 2006. BDIM '06. The First IEEE/IFIP International Workshop, p29 - 36

Sheikhpour, R., Modiri, N., 2012, "A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management", Indian Journal of Science and Technology, Feb 2012, Vol. 5 No. 2

Shein, E, 2015, “Companies Proactively Seek Out Internal Threats”, Communications of the ACM. Nov2015, Vol. 58 Issue 11, p15-17.

Soomro, Z.A., Shah, M.H., Ahmed, J, 2016, “Information security management needs more holistic approach: A literature review”, International Journal of Information Management, Volume 36, Issue 2, April 2016, p215–225

Talla, M. R., Valverde, R., 2012, "Data oriented and Process Oriented Strategies for Legacy Information Systems Reengineering". ACEEE International Journal on Information Technology, Volume 2, Issue 1, p47-51.

Web Articles:

Andersson, S., 2001, "Fröfabriken måste sälja huset för att klara IT-köp", NyTeknik.se as viewed Apr 1, 2016; http://www.nyteknik.se/industri/frofabriken-maste-salja-huset-for-att-klara-it-kop-6473955

Arstad Djurberg, J., 2016, "Ingen kan stordatorer längre – då kallas pensionärerna in", ComputerSweden.idg.se, Mar 10, 2016, as viewed April 9, 2016; http://computersweden.idg.se/2.2683/1.652463/stordatorer-pensionarer

Bergsman, J., 2014, "Should Information Security Report Outside IT?", CEB Global/Blogs, Aug 27, 2014, as viewed Apr 10, 2016; https://www.cebglobal.com/blogs/should-information-security-report-outside-it/

Bossert, O., Richter, W., Weinberg, A., 2015, "Protecting the enterprise with cybersecure IT architecture", McKinsey, March 2015, as viewed Apr 4, 2016;http://www.mckinsey.com/business-functions/business-technology/our-insights/protecting-the-enterprise-with-cybersecure-it-architecture

Bradley, T., 2013, "Dropbox is peeking at your files", CSO Online, Sep 13, 2013, as viewed Apr 5, 2016; http://www.csoonline.com/article/2137123/privacy/dropbox-is-peeking-at-your-files.html

Chacos, B., May 5, 2014, “Antivirus is dead, says maker of Norton Antivirus”, PCWorld, as viewed Jan 11, 2016; http://www.pcworld.com/article/2150743/antivirus-is-dead-says-maker-of-norton-antivirus.html

Christey, R. (Ed.), 2011, “2011 CWE/SANS Top 25 Most Dangerous Software Errors” ,CWE/Sans.org, as viewed Mar 30, 2016; http://cwe.mitre.org/top25/

Clarke T., 2010, “Is there best practice for a server to system administrator ratio?”, Computerworld Australia, 09 July, 2010, as viewed Apr 4, 2016; http://www.computerworld.com.au/article/352635/there_best_practice_server_system_administrator_ratio_/

Coffman, D., 2014, "The case for taking the information security function out from underneath the IT umbrella.", InformationWeek, Bank Systems, Technology, Dec 29, 2014, as viewed April 10, 2016; http://www.banktech.com/security/the-separation-of-information-security-and-it--/a/d-id/1318305

Cox, R., Grosse, E., Pike, R., Presotto, D., Quinlan, S., 2002, “Security in Plan 9”, Proc. of the 2002 Usenix Security Symposium, San Francisco, Ca, US, as viewed Mar 25, 2016, http://plan9.bell-labs.com/sys/doc/auth.html

Div, L., 2015, "Why It's Worth Divorcing Information Security From IT", Forbes, June 22, 2015, as viewed Apr 10, 2016; http://www.forbes.com/sites/frontline/2015/06/22/why-its-worth-divorcing-information-security-from-it/#3ee8f8d379e2

Donohue, B., Jan 5, 2015, “Microsoft Reports Massive Increase In Macros-Enabled Threats”, Threatpost.com, as viewed March 22, 2016; https://threatpost.com/microsoft-reports-massive-increase-in-macros-enabled-threats/110204/

Forsvaret (for Danmark), 2016, “Slædepatruljen Sirius”, Forsvaret.dk, as viewed Apr 5, 2016;http://www2.forsvaret.dk/omos/organisation/arktisk/enheder/sirius/Pages/default.aspx

Gourley, B., Nov 4, 2015, “Does next-generation anti-virus solve the fatal flaws of anti-virus”, Red Canary, as viewed Jan 11, 2016; https://www.redcanary.co/2015/11/04/next-generation-anti-virus-solve-fatal-flaws-anti-virus/

Hardekopf, B., 2015, "The Big Data Breaches of 2014", Forbes, Jan 13, 2015, as viewed Mar 16, 2016; http://www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/#f6250f33a48f

Harris, S., 2006, "Should an organization centralize its information security division?", TechTarget, Nov 2006, as viewed, Apr 10, 2016; http://searchsecurity.techtarget.com/answer/Should-an-organization-centralize-its-information-security-division

Heidelberg, J.H., 2007(1), "Default Deny All Applications (Part 1)", Windowssecurity.com, June 5, 2007, as viewed Apr 10, 2016; http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Default-Deny-All-Applications-Part1.html

Heidelberg, J.H., 2007(2), "Default Deny All Applications (Part 2)", Windowssecurity.com, June 5, 2007, as viewed Apr 10, 2016; http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Default-Deny-All-Applications-Part2.html

Kentritas, S., 2013, “Data Flow & Business Process Modeling For Manufacturing Operations Management”, Whitepaper, Dad.net.au, as viewed Feb 24, 2016; http://www.dad.net.au/Files/White%20Paper_MOM_DAD_v03.pdf

Kirk, J., 2013, "Dropbox takes a peek at files. But it's totally nothing, says Dropbox", IDG News Service, Sep 13, 2013, as viewed Apr 6, 2016; http://www.pcworld.com/article/2048680/dropbox-takes-a-peek-at-files.html

Kresge, N., Weiss, R., 2015, "Volkswagen Drops 23% After Admitting Diesel Emissions Cheat", Bloomberg, Sept 21, 2015, as viewed Apr 6, 2016; http://www.bloomberg.com/news/articles/2015-09-21/volkswagen-drops-15-after-admitting-u-s-diesel-emissions-cheat

Luckerson, V., 2014, "7 Controversial Ways Facebook Has Used Your Data", Time Magazine, Feb. 4, 2014, New York, NY, US, as viewed Apr 5, 2016; http://time.com/4695/7-controversial-ways-facebook-has-used-your-data/

Malm, C., March 6, 2015, “Stor trojanattack mot landstinget - hundratals anställda hemskickade”, IDG.se, as viewed Jan 11, 2016; http://www.idg.se/2.1085/1.614057/stor-trojanattack-mot-landstinget--hundratals-anstallda-hemskickade

Mendrez, R., Dec 22, 2015, “3-in-1 Malware Infection through Spammed JavaScript Attachments”, Trustwave.com, as viewed March 22, 2016; https://www.trustwave.com/Resources/SpiderLabs-Blog/3-in-1-Malware-Infection-through-Spammed-JavaScript-Attachments/

Miller, R., 2009, “How Many Servers Can One Admin Manage?, Data Center Knowledge”, Dec 30, 2009, as viewed Apr 4. 2016; http://www.datacenterknowledge.com/archives/2009/12/30/how-many-servers-can-one-admin-manage/

Mulholland, A., 2015, “IoT; Data Flow Management – the science of getting real value from IoT Data”, Constellation Research, as viewed Feb 25, 2016; https://www.constellationr.com/content/iot-data-flow-management-science-getting-real-value-iot-data

Murphy, E.A., 1949, “Murphy’s Law”, Murphy’s Law Site, US http://www.murphys-laws.com/murphy/murphy-true.html

Møllerhøj, J., Jan 22, 2015, “Sådan blev kommuner udsat of ransomware-angrep”, Version2, as viewed Jan 11, 2016; http://www.version2.dk/artikel/saadan-blev-kommuner-udsat-ransomware-angreb-76563

OWASP, 2013, “OWASP Top 10 Vulnerabilities”, OWASP.org as viewed Mar 30, 2016; http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202013.pdf

OWASP, 2013, “OWASP Top Ten Cheat sheet”, Owasp.org as viewed Mar 30, 2016; https://www.owasp.org/index.php/OWASP_Top_Ten_Cheat_Sheet

Reichenberg, N., Wolfgang, M., 2014, "Segmenting for security: Five steps to protect your network", Network World, Nov 24, 2014, as viewed Apr 15, 2016; http://www.networkworld.com/article/2851677/security0/segmenting-for-security-five-steps-to-protect-your-network.html

Riley, C., Pagliery, J., March 19, 2015, “Target will pay hack victims $10 million”, CNN Money, as viewed Feb 4, 2016; http://money.cnn.com/2015/03/19/technology/security/target-data-hack-settlement/

Salz, L., Sept 25, 2015, “Bluffmail från “PostNord” sprider virus, Malmö Stad drabbat”, Sydsvenskan, as viewed Jan 11, 2016; http://www.sydsvenskan.se/malmo/bluffmejl-spred-virus-i-kommunernas-datorer/

Stafford, J., 2014, Which data governance best practices optimally handle a storm of data?, Techtarget.com, April 2014, as viewed Apr 4, 2016;http://searchsoa.techtarget.com/feature/Which-data-governance-best-practices-optimally-handle-a-storm-of-data

Weil, S., 2010, "How ITIL Can Improve Information Security", SecurityFocus.com/Symantec.com, Dec 22, 2004, Updated: Nov 2, 2010, as viewed Feb 20, 2016; http://www.symantec.com/connect/articles/how-itil-can-improve-information-security

Whittaker, Z, May 5, 2014, “Symantec calls antivirus “doomed”, as security gigants fights for survival”, ZD Net, as viewed Jan 11, 2016; http://www.zdnet.com/article/symantec-calls-antivirus-doomed-as-security-giants-fight-for-survival/

Thesises:

Lindström, J., 2009, “Models, Methodology, and Challenges within Strategic Information Security for Senior Managements”, Ltu, Luleå, SE

Nilsson, I., 1978, "GRÖNLANDSFRÅGAN 1929-1933, En studie i småstatsimperialism.", ACTA UNIVERSITATIS UMENSIS, Umeå, SE

Internal Publications:

Magnusson, L., 2010, “10Saab_Secure_B2B_IT_Activities_V1.00.2_01FEB_ADM001”, Saab Automobile IT Strategy Reports, Trollhättan, SE

Magnusson, L., 2011(2), “09SAAB_Saab Security Approval Process_v1.00.2_14MAR_ADM001”, Saab Automobile IT Strategy Reports, Trollhättan, SE

Meeting Procedings:

(ISC)2 SecureScandinavia 2015, Stockholm, SE

Hart, J., May 19, 2015, Speech, “Virtual World Exposed: Hacking the Cloud”, Gemalto-Safenet, US

Hansen, J., May 19, 2015, Speech, “Defending Against Phishing Attacks: Case Studies and Human Defenses”, PhishMe

Other sources:

Facebook, 2016, “Policy”, Facebook.com, as viewed Apr 6, 2016; https://www.facebook.com/policy.php and https://www.facebook.com/terms

Google, 2016, “”, Google.com, as viewed Apr 6, 2016; https://www.google.com/policies/terms/