Synthesis

International Scientific Conference of IT and Business-Related Research

OPTIMIZING CORPORATE INFORMATION SECURITY MANAGEMENT IN THE POST-"HEARTBLEED" WORLD

OPTIMIZACIJA UPRAVLJANJA ZAŠTITOM INFORMACIJA U PREDUZEĆIMA U ERI NAKON HEARTBLEED-A

Viktor Polić
Webster University Geneva, Route de Collex 15, Bellevue, 1293, Switzerland

Abstract:

An optimal business process is defined as a dynamic process that is able to adapt rapidly to the changing environment and maintain satisfactory level of performance directed towards achieving the predefined set of objectives. Corporate information security management is a business process focused on managing risk that can have adverse effects on vital corporate information and related technology and processes. Rapid evolution of information and communication technology (ICT) and ways it is used to collect, analyze and disseminate information carries many opportunities to improve corporate value chain, but also carries uncertainty and new risks. Unexpected flaws were recently discovered in fundamental building blocks of ICT such as OpenSSL challenging methods used to manage corporate information security. In this paper, we will review information security management process focusing on its risk management component and suggest improvements in order to remain proactive. Suggested improvements will cover methods for assessing and measuring risk in the areas of ICT that were hit by unexpected vulnerabilities such as business application development and integration, establishing corporate information security incident response teams, and developing a framework for exchanging information security threat intelligence.

Key words:

risk management, incident management, vulnerability management, information security risk intelligence.

Apstrakt:

Optimalnim poslovnim procesom smatra se svaki dinamični proces koji se brzo prilagođava pomenama u okruženju i može da održi zadovoljavajući nivo performansi kako bi se realizovali unapred postavljeni ciljevi.Upravljanje bezbednošću informacija unutar preduzeća predstavlja poslovni proces koji je usmeren ka upravljanju rizicima koji mogu negativno uticati na bitne informacije unutar preduzeća kao i na upotrebu tehnologija i procesa u samoj organizaciji. Brz razvoj informacionih i komunikacionih tehnologija (IKT) kao i način na koji se one koriste za prikupljanje, obradu i prenos podataka nose sa sobom brojne mogućnosti za unapređenje korporativnog lanca vrednosti, ali i brojne neizvesnosti i rizike. Neočekivani nedostaci nedavno su otkriveni u osnovnim gradivnim elementima IKT-a poput OpenSSL paketa, i predstavljaju izazov za metode upravljanja bezbednošću informacija unutar preduzeća. U ovom radu razmatra se proces upravljanja bezbednošću informacija sa naglaskom na komponentu upravljanja rizikom i nude predlozi za moguća poboljšanja u cilju očuvanja proaktivnosti. Ona obuhvaju metode za procenu i merenje rizika u oblastima IKT-a koje su pogođene neočekivanim slabostima, poput razvoja i integracije poslovnih aplikacija, uspostavljanje centra za brzu reakciju u slučaju incidenata vezanih za bezbednost informacija, i razvijanje okvira za razmenu informacija o mogućim pretnjama.

Ključne reči:

upravljanje rizikom, upravljanje incidentima, upravljanje ranjivostima (slabostima).

1. INTRODUCTION

Recent massive data breaches illustrate enterprise risk management deficiencies even within large, regularly audited and well-resourced organizations, which have established information security organizational role. There is no specific type of an organization or industry that seems more vulnerable than others. Banks, retailers, health-care, education, public sector, manufacturing etwere all affected. For those that are not it is likely a matter of time when they will discover an existing breach. There are cases like "Shady RAT" when organizations discovered a breach years after it had occurred (Alperovitch, 2011). What is common for most of those organizations is that they have already established information security management role within their organizational structure. That role is usually based on internationally recognized management standards of such a business process. Independent auditors that follow standard methodologies regularly audit the process. The performance of the business process is continuously assessed through the standard management frameworks with defined process strategy, outputs with measurable and comparable objectives, and related activities continuously tracked in regular work-plan meetings coordinated with related business processes. Nevertheless, incidents occur resulting in massive spending on investigations, loss of business opportunities, lengthy and costly legal processes, and damaged reputation. It is impossible to achieve one hundred percent security from all risks. The chain of technical, organizational and procedural controls for information security protection is as strong as its weakest link. These are the facts that all information security professionals unanimously agree upon. However, none of them foresee incidents with such a high impact and with root causes in those areas of control that were assessed as low likelihood and low impact in audit reports and risk registers. In this paper, we will review information security management process focusing on its risk management component and suggest improvements in order to remain proactive.

2. RESULTS AND DISCUSSION

In order to be proactive, information security management has to effectively prevent risk. How is that possible when fundamental building blocks of information security chain of controls are flawed such as cryptographic controls that protect confidentiality and integrity of data in transfer (Bhargavan *et al.*, 2015)? Information security industry reacts quickly when

E-mail: polic@webster.ch

DOI: 10.15308/Synthesis-2015-85-89

such an important vulnerability is discovered. Vendors of security technologies propose temporary workarounds and release patches for vulnerable products, security service providers propose assessments and recommend solutions to fill in gaps. Internal information security teams meet with ICT operations and application development teams and make tactical decisions to mitigate risks where likelihood of occurrence increased due to a newly discovered vulnerability. Unfortunately, not all organizations are ready to address those risks rapidly enough and consequently become victims of malicious attackers in either a targeted or non-targeted, opportunistic attack. Moreover, incidents with massive impact illustrate that many organizations are not prepared to quickly detect an incident and react in a coordinated manner in order to reduce the detrimental effects.

IMPACT OF A DATA BREACH

Understanding the detrimental effects of an information security incident is a starting point towards a better perception of risk and more effective risk treatment plan. Incidents whose impact could be quantified in financial terms are simpler to perceive. Data destruction or modification would require time and effort to restore or in the worst case to recreate. Such an impact could be quantified by using traditional management metrics such as hour/person and related financial terms using hourly rates or service prices. The cost of legal processes could also be monetized using information from previous similar legal cases. The loss of business opportunities can be measured by average daily number of transactions. However, the loss of organizational reputation is more difficult to quantify, and costs of public relations campaigns could be used to estimate the potential cost to repair reputational damage. Business impact analysis is the formal process for the quantification of detrimental effects of incidents. This process is well defined within the Business Continuity Planning (BCP) organizational process. However, BCP process is usually focusing on large scale disasters in practice and does not cover information security incidents. There are more recent industry standards such as ISO/IEC 27031:2011 (Guidelines for information and communication readiness for business continuity), attempt to fill that gap and include information security incidents into the scope of business impact analysis process. Systematic evaluation of potential risk impact for all categories of risk requires collaborative effort of subject matter experts in all functional areas of law, finance, human resources, strategic management, programming and budget, information management including technology management, audit, and other depending on the type of industry sector.

ORGANIZATIONAL STRUCTURE AND POSITION OF INFORMATION SECURITY MANAGEMENT FUNCTION

Majority of large organizations with resources dedicated to managing information security have them still administratively attached to Information and Communication Technology (ICT) departments. Chief Information Security Officer (CISO) reports to Chief Information Officer (CIO). That could create a potential conflict of interest and subjective prioritization of operational rather than risk-oriented governance decisions. Therefore, budgetary allocations could directly restrict certain risk treatment decisions, or present an obstacle in effective communication of risk factors to risk owners. Risk owners are responsible and accountable for making decisions based on risk treatment plan. That would include risk mitigation, risk acceptance, risk transfer, or risk avoidance. Organizations that have experienced information security risk management deficiencies and were victims of massive data breaches address this issue through reorganization and frequently change CISO's role and responsibilities. Unfortunately, after the first significant breach that usually results in assigning CISO administratively to the enterprise risk officer. While that measure resolves some conflicts between operational IT governance and security risk governance, it does not cover all of the above-listed risk categories. Enterprise risk management function is typically situated within finance department and reports to the Chief Finance Officer. Priority is thus given to financial risk and related impact. Moreover, the internal audit function is also typically focused on financial audits and fraud related incidents. Other risks that have high impact in case of data breaches are not necessarily adequately addressed (Van der Meulen & Rivera, 2015). A more effective solution would be to form a risk management committee or risk clearance committee with subject matter experts covering all risk categories identified as significant within the context of the organization. The committee could be advisory or even the decision making body for strategic decisions concerning risk. In case it is an advisory body, it should report to the chief director or board of directors.

INTEGRATION OF IT GOVERNANCE WITH RISK MANAGEMENT

There are several widely adopted risk management frameworks such as NIST 800-37, COSO ERM guidelines, ISACA COBIT, ISO 31000, and other. Methodologies are very similar and could be outlined in the following activities:

- Risk identification,
- Risk evaluation,
- Risk treatment,
- Risk monitoring.

This is typically a continuous business process in the form of plan-do-check-act-improve.

In order to have an effective information security risk management, it is necessary to integrate it into the information security management process and align it to the enterprise risk management framework as previously stated. Two recently updated information security management frameworks illustrate that the industry has recognized this requirement. ISO/IEC 27001 – Information security management was updated in 2013 to improve evaluation and measurement of the process performance including alignment of information security risk management with ISO 31000 framework (ISO, 2013). ISACA Control Objectives for Information and Related Technology (COBIT) is the framework for the governance of enterprise IT. It was also updated to version 5 with integrated risk management framework that was previously defined as separate framework (ISACA Risk IT) and with integrated evaluation framework (Val IT) (ISACA, 2012). For instance, COBIT 5 defines the approach to information governance as an enabler with performance measurement using metrics for goal achievement (Lag Indicators) and metrics for application of practice (Lead Indicators). It should be a strategic goal of Information Security Management functions to transform itself to business enablers rather than to remain perceived as business obstacles.

SHIFT RISK ASSESSMENT FOCUS TO INFORMATION AND PEOPLE

Effectiveness of information security controls is typically assessed by covering different categories of controls as defined within standards such as ISO/IEC 27002:2013 Code of practice

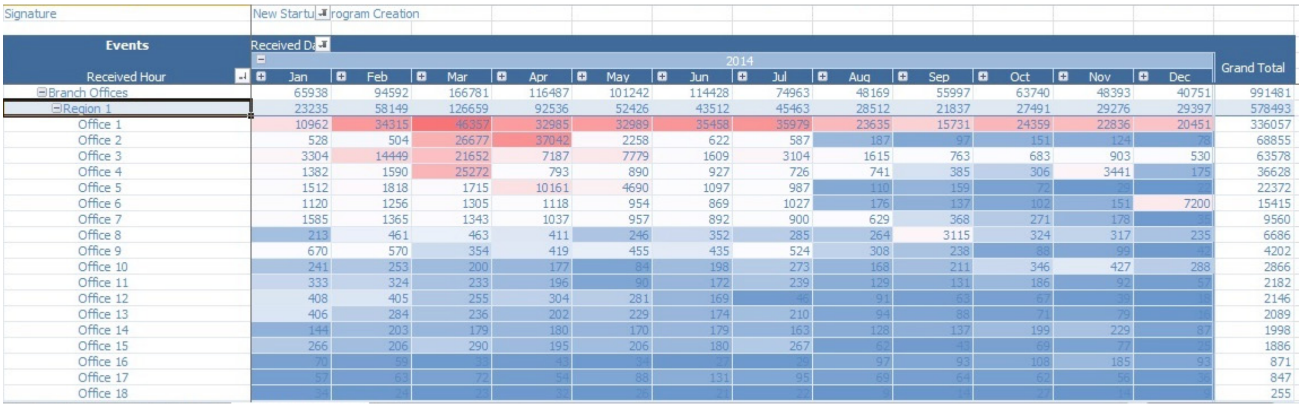
DOI: 10.15308/Synthesis-2015-85-89

for information security controls (ISO, 2013a). In practice, this is a periodic assessment either as part of an audit or as assessment for obtaining certification. Continuous assessment of all control areas for monitoring of risk indicators is not practical and would represent significant cost. Areas that are traditionally continuously monitored are related to IT performance indicators (operational controls), network perimeter security controls (network firewalls, Internet proxies), anti-malware protection (end-point anti-virus systems, data streaming anti-virus systems) and e-mail protection (anti-spam systems). Database and application security is typically focused on access controls within authentication, authorization and accounting protection systems. Host hardening practice would include configuration and change management monitored by vulnerability scanning systems. However, these controls are inefficient to prevent targeted attacks based on advanced persistent threats (APT), or attacks on personal computers of end-users or vulnerable servers that are used for bouncing to other systems that host more critical data. Security information and event management (SIEM) systems could effectively detect network intrusion attempts but less likely intrusions mentioned above. The reason for this is that SIEMs typically come with predefined set of rules, data correlation algorithms, and attack signatures that are not significant for certain organizational specific risks. In more accurate scenarios, they are configured with custom set of rules and data sources selected in the business context and risk context defined within the earlier suggested risk management framework. The most advanced systems are custom designed data analytics systems based on online analytical processing (OLAP) for information security intelligence. Reinforced with machine learning algorithms, they could be transformed to systems that search for uncertain rather than traditional systems that are looking for certain (known patterns vs. unknown patterns) events. In addition, OLAP data structures are optimized for analytical activities (data reading) rather than data maintenance (data modifications). They are meta-data based on dimensions and could provide storage for much larger sets of data with longer retention plan (years rather than months). Data are stored in multidimensional cubes with dimensions such as time, host and categories of security events, and measures (facts). Each dimension could be drilled through in the near real-time. For instance, hosts could be subdivided into servers, networks, devices, laptops, desktops, smart phones, and further down to details such as MAC address, IP address, process, and BIOS version. Security events could be divided into subcategories such as virus detection, Trojan detection, buffer overflows, RPC calls, and similar. Examples included in this paper are based on the data collected from sources such as commercial endpoint protection suites that include anti-virus, host-based intrusion prevention systems (HIPS), access control systems and other modules and are installed on Windows based servers and personal computers. The population size includes 8524 hosts over the period of three years of data collection. Maximum of 4000 hosts are active at any point in time.

When there is no solid hypothesis about potential security event, either descriptive or prescriptive analytical models could be applied to such data structures. Predictive data mining would be based on the analysis such as sample variance analysis. Descriptive data mining represents a drill-down technique of searching through data to identify potential information security incidents. For instance, searching for "zero-day" viruses would be performed as the analysis of data on the particular event from HIPS module such as "New startup program creation" as illustrated in Figure 1.

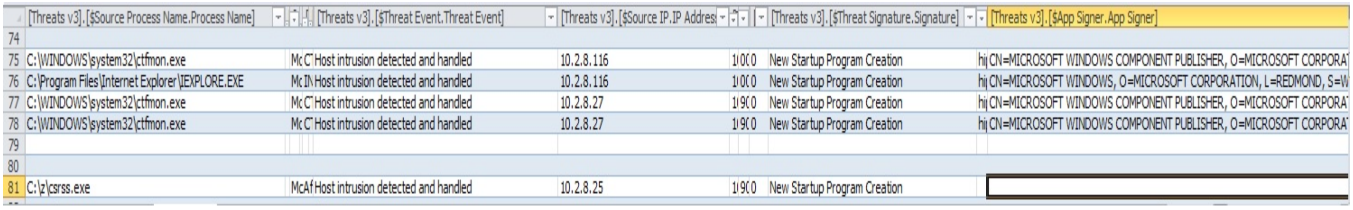
Drilling into red-colored cells of the above-given table would display details of all source processes on each host that have generated that specific HIPS event. Filtering out processes that have a valid digital code signature would reveal potentially infected files. In this specific example, we were able to identify a polymorphic form of a virus that hides behind a well-known Windows client server runtime system process CSRSS.EXE as illustrated in Figure 2.

An example of predictive data mining would be the analysis of the number of attempted HTTP sessions detected by Internet proxy servers. Figure 3 illustrates plot of distance from means of "usual behavior" in Web usage. The host with the largest distance from the mean was infected with a "zero-day" virus. "Zero-day" viruses are unknown to signature based anti-virus systems.



Signature	New Startu rogram Creation												
Events	Received Da												
	2014												Grand Total
Received Hour	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	
⊟Branch Offices	65938	94592	166781	116487	101242	114428	74963	48169	55997	63740	48393	40751	991481
⊟Region 1	23235	58149	126659	92536	52426	43512	45463	28512	21837	27491	29276	29397	578493
Office 1	10962	34315	46357	32985	32989	35458	35979	23635	15731	24359	22836	20451	336057
Office 2	528	504	26677	37042	2258	622	587	187	97	151	124	78	68855
Office 3	3304	14449	21652	7187	7779	1609	3104	1615	763	683	903	530	63578
Office 4	1382	1590	25272	793	890	927	726	741	385	306	3441	175	36628
Office 5	1512	1818	1715	10161	4690	1097	987	110	159	72	29	22	22372
Office 6	1120	1256	1305	1118	954	869	1027	176	137	102	151	7200	15415
Office 7	1585	1365	1343	1037	957	892	900	629	368	271	178	35	9560
Office 8	213	461	463	411	246	352	285	264	3115	324	317	235	6686
Office 9	670	570	354	419	455	435	524	308	238	88	99	42	4202
Office 10	241	253	200	177	84	198	273	168	211	346	427	288	2866
Office 11	333	324	233	196	90	172	239	129	131	186	92	57	2182
Office 12	408	405	255	304	281	169	46	91	63	67	39	18	2146
Office 13	406	284	236	202	229	174	210	94	88	71	79	16	2089
Office 14	144	203	179	180	170	179	163	128	137	199	229	87	1998
Office 15	266	206	290	195	206	180	267	62	43	69	77	25	1886
Office 16	70	59	33	43	34	37	29	97	93	108	185	93	871
Office 17	57	63	72	54	88	131	95	69	64	62	56	36	847
Office 18	34	24	23	32	26	21	22	9	14	27	14	9	255

Figure 1."New startup program creation" events from PCs in branch offices over one year



	[Threats v3].[$Source Process Name.Process Name]		[Threats v3].[$Threat Event.Threat Event]	[Threats v3].[$Source IP.IP Addres		[Threats v3].[$Threat Signature.Signature]		[Threats v3].[$App Signer.App Signer]
74								
75	C:\WINDOWS\system32\ctfmon.exe	Mc C'	Host intrusion detected and handled	10.2.8.116	1 0(0	New Startup Program Creation	hi	CN=MICROSOFT WINDOWS COMPONENT PUBLISHER, O=MICROSOFT CORPORA
76	C:\Program Files\Internet Explorer\IEXPLORE.EXE	Mc IN	Host intrusion detected and handled	10.2.8.116	1 0(0	New Startup Program Creation	hi	CN=MICROSOFT WINDOWS, O=MICROSOFT CORPORATION, L=REDMOND, S=W
77	C:\WINDOWS\system32\ctfmon.exe	Mc C'	Host intrusion detected and handled	10.2.8.27	1 9(0	New Startup Program Creation	hi	CN=MICROSOFT WINDOWS COMPONENT PUBLISHER, O=MICROSOFT CORPORA
78	C:\WINDOWS\system32\ctfmon.exe	Mc C'	Host intrusion detected and handled	10.2.8.27	1 9(0	New Startup Program Creation	hi	CN=MICROSOFT WINDOWS COMPONENT PUBLISHER, O=MICROSOFT CORPORA
79								
80								
81	C:\z\csrss.exe	McAf	Host intrusion detected and handled	10.2.8.25	1 9(0	New Startup Program Creation		

Figure 2. Searching for unsigned process that triggered HIPS event

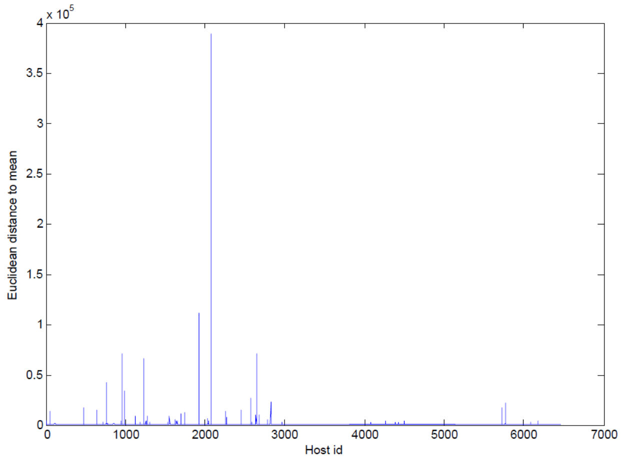


Figure 3. Searching for computers infected with "zero-day" viruses

Behavior analysis would require multidimensional analysis where dimensions could be categories of visited or blocked web-sites. Behavior could be clustered by observing numbers of nodes within the clusters and changes of trends in the distance of a cluster from sample means. Figure 4 illustrates the observation of trends, and significant clusters to analyze would be clusters 9 and 14 where the trend changes. It is also important to note that the error is smaller with larger number of clusters in the analysis. This reduces uncertainty and drilling into data within significant clusters would discover attempts to access Web-site non-compliant to the security policy. Behavior analysis could also help in distinguishing between human Web usage and automated Web usage by malicious bots. Bots are hosts infected by malware attempting to communicate to command and control servers of a botnet or a network used to perform spamming or DDoS attacks.

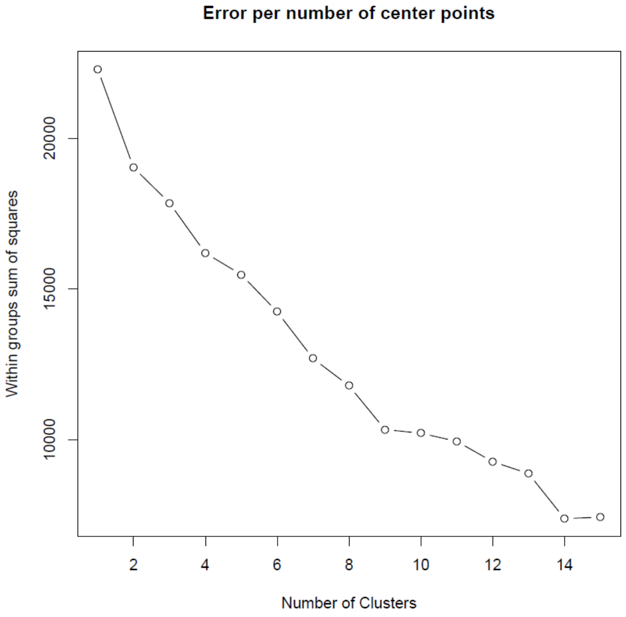


Figure 4. Clustering nodes by Web usage

Developing in-house skills and tools to shift focus of information security management to risk areas that are more vulnerable to high impact incidents such as individual computers or even mobile devices significantly shortens the time to detect events that could lead to incidents. Further development might involve implementation of neural networks and supervised or even non-supervised learning to achieve forecasting of risk trends.

DEVELOPING RISK INTELLIGENCE

Information security professionals should stay away from sensationalism related to public disclosure of vulnerabilities such as "Heartbleed" (CVE, 2014), "Poodle"(Möller *et al.*, 2014), and similar. They should drill down to the root of the issue and rationally evaluate own risks. The most critical issue with the "Heartbleed" bug is not that parts of the memory captured may contain some information. The real problem is that it should never contain such sensitive information such as the server's private cryptographic key. The answer is in the implementation of the RSA. The emphasis is on the word "implementation" and not on the design of a cryptographic algorithm. The emphasis should be placed on the quality of implementation. There are many software implementations of cryptographic primitives. Implementation should undergo security assessment such as static and dynamic code analysis, and fuzzing. Figure 5 illustrates the type of risk assessment that should be performed to verify the level of protection of cryptographic controls and relative significant vulnerabilities disclosed over the past year. High impact vulnerabilities in the basic building block of protection controls are not new or recent. Wired Equivalent Privacy was flawed with vulnerability in RC4 algorithm similar to "Poodle" already back in 2001 (AlFardan *et al.*, 2013). In 2007, NIST 800-90a specified the standard for random number generator (Dual_EC_DRBG) that was vulnerable (Schneier, 2007). Regardless of the fact that the vulnerability was deliberately left within the standard or accidental lack of security assessment, it illustrates together with more recent vulnerability disclosure that not even the industry standards should be taken for granted and that security assessment must be an integral part of system development and integration, or else organizations will continue to operate with a false sense of security until they realize that they are a victim of a security breach.

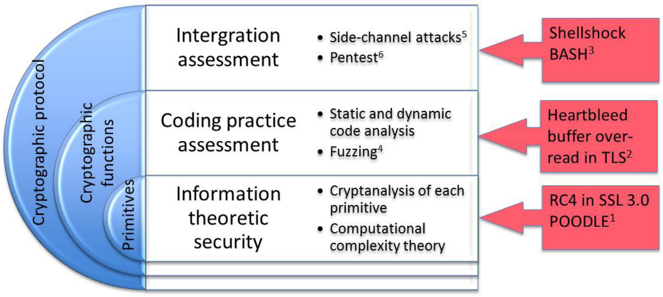

Cryptographic protocol
Cryptographic functions
Primitives
Intergration assessment
Side-channel attacks5
Pentest6
Coding practice assessment
Static and dynamic code analysis
Fuzzing4
Information theoretic security
Cryptanalysis of each primitive
Computational complexity theory
Shellshock BASH3
Heartbleed buffer over-read in TLS2
RC4 in SSL 3.0 POODLE1

Figure 5. Cryptographic controls risk analysis

3. SUMMARY

Risk intelligence is not an in-house task. Intelligence is at the highest level of abstraction and represents the ability to perceive and retain knowledge. Risk intelligence would involve intelligence on threats, vulnerabilities, impact, and likelihood of risk occurrence. If an organization has enough historical data, it may attempt to build in-house risk intelligence. Unfortunately, there are so many unknowns related to information security risks that all of the above-mentioned risk components should be measured, compared and analyzed across similar industries, regions, security postures and many other classes of data sources. While

DOI: 10.15308/Synthesis-2015-85-89

there are standardized enumerations for vulnerabilities (CVE, 2014a) and impact could be quantified as discussed earlier, data threats are already more difficult to compare. Technical threats related to known attacks on computer systems such as network addresses, intrusion detection signatures, and similar are comparable. However, each organization should build its own threat intelligence through the above described security data mining. For those risks present in all components comparable, Key Risk Indexes (not indicators) could be established and monitored at the level of industry similar to stock market indexes. They could represent weighted average of incident occurrence due to comparable selected risk parameters. Empowered with risk intelligence, the risk management committee would be in a position to make sound strategic risk decisions and maintain proactive information security.

Acknowledgements. Special thanks to Mr. Jose Nicolas Velasquez Orozco for developing plots for Figures 3 and 4.

REFERENCES

AlFardan, N., *et al*. (2013). *On the Security of RC4 in TLS and WPA*. Retrieved from http://www.isg.rhul.ac.uk/tls/

Alperovitch, D. (2011). *Revealed: Operation Shady RAT*. Retrieved from http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

Bhargavan, K., Fournet, C., Delignat-Lavaud , A., *et al*. (2015). *Freak: Factoring RSA Export Keys*. Retrieved from https://www.smacktls.com/#freak

CVE. (2014). *CVE-2014-0160*. Retrieved from https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160

CVE. (2014a). *About Common Vulnerabilities and Exposures*. Retrieved from https://cve.mitre.org/about/

ISACA. (2012). *What is COBIT 5*? Retrieved from http://www.isaca.org/cobit/pages/default.aspx

ISO. (2013). *ISO/IEC 27001 :2013 Information security management*. Retrieved from http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

ISO. (2013a). *ISO/IEC 27002: 2013 Code of practice for information security controls*. Retrieved from http://www.iso.org/iso/catalogue_detail?csnumber=54533

Möller, B., Duong, T., & Kotowicz, K. (2014). *This POODLE Bites: Exploiting The SSL 3.0 Fallback*. Retrieved from https://www.openssl.org/~bodo/ssl-poodle.pdf

Schneier, B. (2007). *Did NSA Put a Secret Backdoor in New Encryption Standard*? Retrieved from http://archive.wired.com/politics/security/commentary/securitymatters/2007/11/securitymatters_1115

Van der Meulen, R., & Rivera, J. (2015). *The emergence of digital risk and digital risk officer, Gartner*. Retrieved from http://www.gartner.com/newsroom/id/2794417

DOI: 10.15308/Synthesis-2015-85-89