"Mircea cel Batran" Naval Academy Scientific Bulletin, Volume XIX – 2016 – Issue 2
The journal is indexed in: PROQUEST / DOAJ / Crossref / EBSCOhost / INDEX COPERNICUS / DRJI / OAJI / JOURNAL INDEX / I2OR / SCIENCE LIBRARY INDEX / Google Scholar / Academic Keys/ ROAD Open Access / Academic Resources / Scientific Indexing Services / SCIPIO / JIFACTOR

PEOPLE, PROCESS, AND TECHNOLOGY; A BLEND TO INCREASE AN ORGANIZATION SECURITY POSTURE

Vlad-Mihai COTENESCU[1]

[1] Eng. Military Technical Academy, Bucharest, Romania

Abstract: *Few would argue that enterprises have increasingly become dependent on IT to facilitate business operations. In today's knowledge-driven economy, information is critical to an enterprise's ability not only to survive but also to thrive. Experienced business leaders know that information deserves at least the same level of protection as any other asset, and have made information security managers a common addition to the organization chart.*
Organizations lose proprietary information daily due to hackers, insiders, or business partners. Most organizations think that this issue isbeing addressed with technology alone, but that is not realistic. This article will try to demonstrate that focusing holistically on people, processes, andtechnology can reduce the impact of data loss. People can be trained to recognize threats such asphishing and social engineering. Processes can address the issue through policies and procedures.Technology can be implemented to monitor and prevent attacks against the environment.

Introduction:

Organizations always faced the problem of dealing with cyber-attacks. In nowadays computer networks became very complex and data is not only stored in private datacenters. With the introduction of cloud computing, more and more organizations start to migrate to public clouds trying to benefit from the benefits of this solution. By doing so, they leave themselves open to attacks as the systems are accessible from the Internet. Data is under the control of the cloud provider and the organization has little or no visibility on to what happens in the public cloud network infrastructure. Cloud storage has introduced storing corporate data externally with companies such as Dropbox, YouSendIt, and Box.net. These all create vulnerabilities that can be exploited.

With new technological capabilities come new threat vectors to corporate data. Mobile computing hasintroduced the new problem of corporate data being stored on mobile phones and tablets. BYODhas for the first time introduced the threat of corporate data on user's personal devices.

If no action is taken to reduce the impact of data loss an organization could easily go outof business. "Ideas, patents, and inventions are routinely stolen. Companies have closed beforerealizing that the sudden competition that ran them out of business resulted from their own stoleninformation" (Grimes, 2012). To reduce this risk, organizations must take action by focusingtheir efforts on people, process, and technology.

Hypothesis:

Everyone thinks that cyber-attacks can be stopped solely using technology and it's only an IT problem but that is far from the truth. There isn't, yet, a silver bullet when it comes to these issues and in order to increase the security level of an organization a blend of technology, people and processes needs to be created.

Users who have access to the data are often the root cause of the data loss. Employees opening an email whichlaunches malicious code, data on a lost thumb drive, sending confidential data via email, orinnocently connecting to a malicious website all demonstrate that the human element is a majorfactor in the data loss problem and must first be controlled before the technology can make adifference.

The lack of appropriate processes is another factor resulting in data loss. If there are no data usage policies or secure transmission procedures in place data will be lost (Ernst & Young,2011). The factors coupled with the lack of data usage monitoring can create the perfect storm.

In order to have the right protections in place, you would need to look at how security breaches are occurring and what are their sources. All data breaches start with a precipitating event which results in data loss. "Entities that cause or contribute to an incident are known as threat agents" (Verizon, 2012, p. 16). These threat agents vary and have different approaches. "Actions performed by them can be maliciousor non-malicious, intentional, or unintentional, causal or contributory, and stem from a variety of motives" (Verizon, 2012, p. 16). Verizon identifies, "three primary categories of threat agents – External, Internal, and Partner" (Verizon, 2012, p. 16). Figure 1 below shows the threat agents over time by percent of breaches:

DOI: 10.21279/1454-864X-16-I2-057

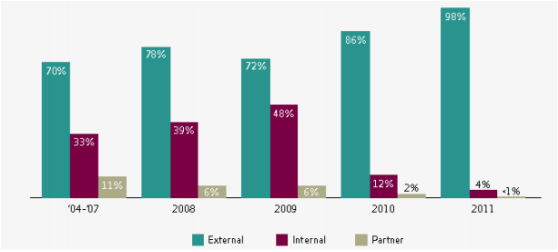

Figure 1. Threat agents over time by percent of breaches, by (Verizon, 2012, p.16)

There are various types of avenues that can be followed in order to exploit internal threats.

The insider threat, whereby an employee acts, knowingly or unknowingly, in a counter-productive way to cause significant damage to an organization, has become a key risk for organizations around the world. This is in part driven by the greater access individuals have to critical information and systems as organizations become more and more connected. In addition, ever more sophisticated methods of carrying out a cyber-attack and the availability of more outlets for leaking information are increasing the threat.

Insiders who have advanced rights to systems can be considered very dangerous to an enterprise. These individuals have the ability to delete business information, destroy backup tapes, install viruses, make modifications to public facing websites, and shut down systems.

Individuals who work on the inside often have the opportunity to use information systems to steal intellectual property. “This category includes industrial espionage involving insiders;information stolen often includes proprietary engineering designs, scientific formulas, sourcecode, and confidential customer information” (Capelli et al., 2012, p. 5). Thefts of this naturecan and do cripple organizations financially and competitively in the marketplace.

Insider fraud can be defined as employees accessing information systems with the intent to modify or delete the data for financial gain. This can entail selling personal information such ascredit card numbers, social security numbers or health insurance ID numbers, users modifyingrecords; or stealing money directly from a bank, store, or the federal government (Capelli et al.,2012, p. 4). This threat will often go unnoticed for long periods of time depending on how smartthe insider is; small changes often go unnoticed until an audit.

To help manage the insider threat, organizations employ good security people; systems log behavior from physical access to the use of IT systems and software monitoring tools analyze the logs and generate alerts. Yet, in many cases, this is not working: there are frequent reports of successful attacks on the same organizations that apparently deploy all these defenses. Where people risk is concerned, there seems to be a blind spot.

Internal threats don’t need to be always performed by bad intentioned people. Sometimes human errors can lead to damages that are equally or even more destructive to an organization. Often users simply make mistakes and as a result data is lost. Users inadvertently send sensitive emails to the wrong email address, lose laptops, USB drives, smartphones, printouts, or backup tapes with proprietary or protected data while traveling or in transit to an outside meeting.

External Threats

The external threat originates from outside the organization. These threats are carried outby “former employees, lone hackers, organized criminal groups and government entities”(Verizon, 2012, p. 16). Much of the recent activity seen has been with Hacktivist groups such asAnonymous and LulzSec.

These attacks can be carried out from anywhere in the world and can be really hard to be traced to the source. Some attacks that can be destructive are DDoS, SQL Injection, XSS, weak passwords or RATs (Remote access Trojans) planted using Phishing emails or Social Engineering.

Partner Threat

Partner threat is based on business relationships with third parties with whom data isshared and lost due to human error or fraudulent activity. “This includes suppliers, vendorshosting providers, outsourced IT support, etc. A level of trust and privilege is usually impliedbetween business partners” (Verizon, 2012, p. 16). This form of data loss is difficult to control asonce the data leaves the organization oversight is lost.

In order to protect the organization against all these threats a very good information security strategy needs to be put in place. This enterprise strategy needs to be based on the identified risks to the organization and must explore potential avenues that can be used to exploit these risks. In order identify the most important assets or data you would need to involve system, business and data owners. This group of people together with information security personnel can identify appropriate mitigation strategies that need to be implemented.

To address the human factor of the problem an organization needs to have a very solid security awareness program that helps them understand the threats that they are facing and also what processes are in place to help respond to different problems (i.e. incident response process)

DOI: 10.21279/1454-864X-16-I2-057

Technology is equally important in this equation as it can be leveraged to put to use processes and it also can deliver useful information to the human aspect.

In the same time, vendors need to be properly selected and managed to make sure they have security controls in place that can prevent putting at risk the organization. At the same time, it is important to have monitoring controls in place that will allow detecting any attacks coming in from the partner or if any data is being exfiltrated.

BIBLIOGRAPHY:

[1] Capelli, D., Moore, A., &Trzeciak, R. (2012). The cert guidetoinsiderthreats: howtoprevent, detect, andrespondtoinformationtechnologycrimes(theft, sabotage, fraud). UpperSaddle River, NJ: PearsonEducation, Inc.

[2] Cisco. (n.d.). Cisco ASA 5500 series adaptive securityappliances. Retrievedfrom http:// www.cisco.com/en/US/products/ps6120/index.html

[3] Databreaches.net. (2011, December 14). I can just picture it. Retrievedfrom http:// www.databreaches.net/?p=22173

[4] Dealingwith data security. (2012, June 22). Top 6 data breaches for 2012, thus far. Retrievedfrom http://datasecurityweekly.com/top-6-data-breaches-for-2012-thus-far/

[5] Ernst, & Young. (2011, October). Data lossprevention: keepingyoursensitive data out of thepublic domain [White Paper].

[6] SANS Institute (2012, Novmber 07). People, Process, and Technologies Impact onInformation Data Loss. Retrievedfromhttps://www.sans.org/reading-room/whitepapers/dlp/people-process-technologies-impact-information-data-loss-34032

DOI: 10.21279/1454-864X-16-I2-057