The Cyber Threat Risk – Oversight Guidance for CEOs and Boards

By:
Christopher Petersen
CTO & Co-Founder of LogRhythm

With a Foreword By:
Sameer Bhalotra
Former White House Senior Director for Cybersecurity

THE TIME HAS come for CEOs and Boards to take personal responsibility for improving their companies' cyber security. Global payment systems, private customer data, critical control systems, and core intellectual property are all at risk today. As cyber criminals step up their game, government regulators get more involved, litigators and courts wade in deeper, and the public learns more about cyber risks, corporate leaders will have to step up accordingly.

Sameer Bhalotra

Former White House Senior Director for Cybersecurity

Introduction

At the height of the critically important holiday shopping season in 2013, one of North America's largest merchants suffered a major data breach. Cyber thieves surreptitiously compromised point-of-sale (POS) systems and stole the payment card data of 40 million customers, along with non-payment personal data of another 70 million customers.[1] In terms of the amount of sensitive information stolen, this was among the largest known data breaches in history.

The fallout from this event was swift and sobering. The company's shares initially plunged 11% following the announcement of the breach. Sales fell 3.8% as the number of transactions dropped 5.5% during the crucial holiday season.[2] Q1 2014 earnings dropped 16%.[3] By the second quarter of 2014, the company reported net pre-tax data breach expenses of $129 million, or 13 cents per share—and that was just the beginning.[4] Even now, expenses continue to mount as the company prepares for class action and other lawsuits while paying for credit monitoring for tens of millions of customers.

CEOs need to elevate the importance of cyber security and be more directly involved in setting the level of acceptable risk.

The data theft and the ensuing loss of confidence took a toll on the company's executive ranks. The CIO resigned three months after the breach announcement, and the CEO lost his job three months later, due in part to the disastrous effects of the breach. Institutional Shareholder Services urged shareholders to vote out the directors who served on the audit and corporate responsibility committees, claiming that the committee members' failure to ensure appropriate management of these risks set the stage for the data breach that resulted in significant losses to the company and its shareholders.[5]

This particular breach is being felt far beyond the company at the heart of it. Banks and credit unions have spent more than $200 million to date replacing credit and debit cards for consumers whose accounts were compromised. This single breach alone affected 10% of the debit and credit card customers of every bank and credit union in the U.S.[6] While consumers aren't directly liable for any financial losses due to fraud that results from this event, the financial institutions that typically absorb credit card fraud are likely to sue the victimized merchant to recover breach-related costs.

Beyond this singular event, recent breaches of some of the largest financial institutions in the U.S. are garnering attention at the highest levels of government. President Obama and his top national security advisors have received briefings on the cyber attacks on JP Morgan Chase and nine other financial companies. Corporate executives with those financial institutions are expected to cooperate with the U.S. Secret Service as the agency explores the details of the breaches in search of the criminal actors and their motives.

These and other attacks headlining business news reports demonstrate the imperative for CEO and Board level involvement in IT security. CEOs need to elevate the importance of cyber security and be more directly involved in setting the level of acceptable risk. The state of an organization's IT security posture is too important to be fully delegated to the CIO and CISO and then disregarded at the CEO level. A serious cyber attack can have a material adverse effect on a company's financial well being, and this places cyber security into the category of a business risk that warrants CEO and Board attention.

[1] Brian Krebs, "The Target breach, by the numbers," May 14, 2014

[2] Paul Ziobro, "Target Earnings Slide 46% After Data Breach," The Wall Street Journal, updated February 26, 2014

[3] James Covert, "Target data crisis haunts Q1 earnings, with 16% drop," New York Post, May 21, 2014

[4] Press release, "Target Reports Second Quarter 2014 Earnings," August 20, 2014

[5] Paul Ziobro, "ISS urges overhaul of Target board after data breach," The Wall Street Journal, May 28, 2014

[6] A letter to the U.S. Senate from William Hughes, Senior Vice President, Government Affairs, Retail Industry Leaders Association, February 3, 2014

A tangible step the executive leadership can take is to ensure that the budget set aside for strategic security spending is used to invest in cyber security practices that are most relevant to today's advanced attacks. The analyst firm Gartner strongly advocates a rebalancing of the cyber security budget, shifting significant funds from pure prevention to detection and response.

Neil MacDonald, vice president, distinguished analyst and fellow emeritus at Gartner Inc., wrote, "In 2020, enterprise systems will be in a state of continuous compromise. They will be unable to prevent advanced targeted attacks from gaining a foothold on their systems. Unfortunately, most enterprise information security spending to date has focused on prevention, in a misguided attempt to prevent all attacks." He adds, "We believe the majority of information security spending will shift to support rapid detection and response capabilities, which are subsequently linked to protection systems to block further spread of the attack." MacDonald's report includes a key recommendation: "Invest in your incident response capabilities. Define and staff a process to quickly understand the scope and impact of a detected breach."[7]

The Security Intelligence Objective

Let's consider that major merchant breach of 2013 once again. Once the event was discovered – by outsiders, no less – weeks of deep forensic investigations into the cause of the security breach ensued. Perhaps the most stunning revelation of all is that prior to the disastrous theft of the sensitive information, the company was receiving digital warning signs that something was amiss with the point-of-sale system. Months earlier, the merchant had installed a $1.6 million malware detection system that correctly identified and alerted on the attackers' suspicious activity on multiple occasions. However, the company failed to follow-up on these security alerts.[8]

Prior to the disastrous theft of the sensitive information, the company was receiving digital warning signs that something was amiss.

Weeks prior to the POS compromises, it is suspected the credentials of an HVAC vendor were compromised. These credentials were used to gain initial access to the IT environment, allowing the cyber criminals to perform reconnaissance and stage their attack.

Had the company been able to detect the compromised credentials, the subsequent internal reconnaissance activities, or the eventual installation of malware on POS systems, it could have prevented the breach; instead the company was unable to see the early warning signs and ignored subsequent alerts. This begs the question, "Why didn't the merchant pursue the alerts?" The company itself acknowledged that they effectively misinterpreted the early warning signs.

If collecting data from existing security systems, correlating that data in a single repository and raising frequent alerts to trained security professionals is insufficient to detect and prevent or at least stop breaches, then exactly what is necessary to do the job? This is the question being raised by every organization with a mandate to protect its customer data, its intellectual property, its trade secrets and business strategies, and ultimately its market value.

[7] Neil MacDonald, Gartner, Inc., Prevention is Futile in 2020: Protect Information Via Pervasive Monitoring and Collective Intelligence, 30 May 2013

[8] Michael Riley, Ben Elgin, Dune Lawrence, and Carol Matlack, "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It," Bloomberg Businessweek, March 13, 2014

Detecting Threats that Present a Danger

Practically every business entity – public or private; small, medium or large; across every industry sector – is subject to cyber attacks today. Such attacks now take place on an industrial scale. PwC's annual Global State of Information Security Survey for 2015 shows that the compound annual growth rate of detected security incidents has increased 66% year-over-year since 2009. Survey respondents acknowledge detecting a total number of 42.8 million security incidents in 2014—an increase of 48% over incidents detected the previous year. That's the equivalent of 117,339 incoming attacks per day, every day, and that's only what has been detected and reported. One cyber security firm recently estimated that as many as 71% of compromises go undetected.[9] The problem is now so acute that more than half of U.S. companies regard the threat from cyber attacks as one of their top three business risks.[10]

Organizations must clear this fog of noise to bring visibility to the threats that matter—those that present material risk and which require a prompt response.

In most organizations, various security sensors provide a continuous stream of threat related events; for example, patterns of activity on the network that seem out of character for the business. Most companies have invested in detection technologies that uncover threats at the rate of thousands of events per hour, or even thousands per minute in large enterprises.

This constant stream of threat data effectively overwhelms security teams in a fog of noise. Consequently, detecting which underlying threats pose actual risk and require further investigation is made difficult, if not impossible, for most organizations. This is further complicated by the fact that some threats can't be detected by traditional security sensors and require different approaches entirely.

Organizations must clear this fog of noise to bring visibility to the threats that matter—those that present material risk and which require a prompt response. This is the role of Security Intelligence.

Business Intelligence has helped numerous organizations clear the fog of too many points of seemingly extraneous business data to find previously unseen opportunities for a competitive advantage. Security Intelligence does much the same thing with threat information, enabling organizations to clearly see the threats that matter so they can respond quickly to mitigate the risk. The main objective of Security Intelligence is to deliver the right information, at the right time, with the appropriate context, to significantly decrease the amount of time it takes to detect and respond to potentially damaging cyber threats.

[9] PwC, The Global State of Information Security Survey 2015, www.pwc.com/gsiss2015

[10] BAE Systems, Business and the Cyber Threat: The Rise of Digital Criminality, February 2014

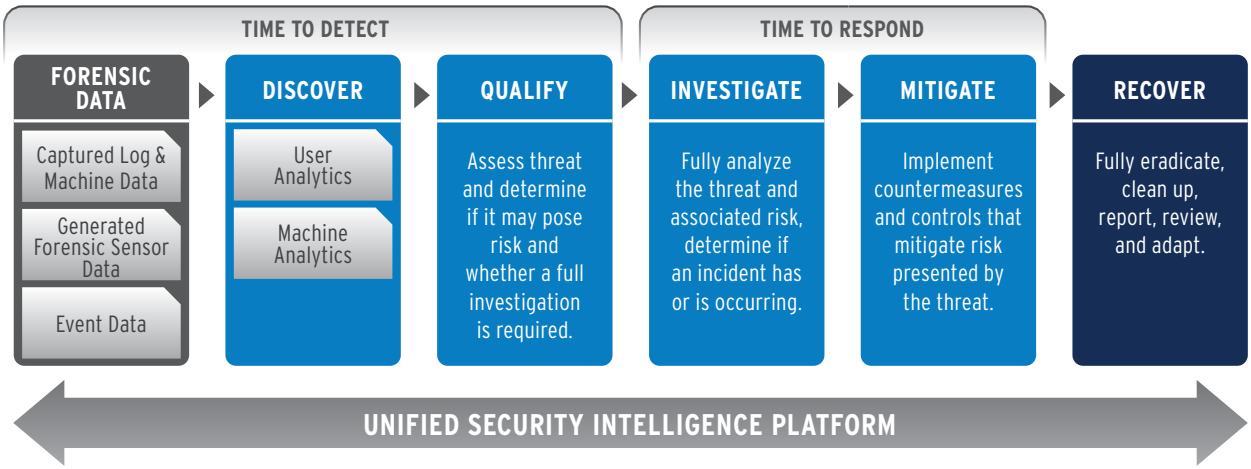
Responding to Threats

Effective IT security depends on skilled people, well defined policies and processes, and a range of integrated technologies. As both the volumes of cyber threats and the sophistication of attack methods continue to grow, security technology is critical in augmenting the human expertise necessary to successfully detect and respond to potentially damaging threats.

Cyber threats are evidenced in underlying forensic data. Forensic data consists of the log and machine data being constantly generated by every server, device, application, database, and security system deployed across the IT environment. Additional forensic visibility is achieved via the deployment of targeted forensic sensors that can gather deep visibility across servers, endpoints, and entire networks. Within this massive data set are clear indicators of threats. The role of Security Intelligence is to unlock the insight contained within this data, helping organizations clearly identify those threats that could cause damage and present actual risk, and facilitating end-to-end threat detection and response™.

Organizations that want to maintain a strong security posture must invest in a more robust and heavily automated, end-to-end threat detection and response capability. This capability can be described as a progression of stages:

Figure 1: The end-to-end threat detection and response lifecycle™



Across the end-to-end threat detection and response process, there are two key metrics organizations should measure and strive to improve: their Mean-Time-to-Detect™ (MTTD™) and Mean-Time-to-Respond™ (MTTR™).

- MTTD is the average amount of time it takes an organization to discover and qualify those threats that could potentially impact the organization.
- MTTR is the average amount of time it takes an organization to fully investigate the threat and mitigate any risk presented.

Unfortunately, many organizations operate in a mode where MTTD and MTTR are measured in weeks or months. In 2013, Verizon reported that 66% of the breaches they investigated as part of their annual breach study took months or years to discover. Months of going undetected by the breached organization enables an attacker to establish a foothold on the organization's network and begin, if not complete, his malicious mission. Therefore companies seeking to reduce their cyber security risk must minimally move the MTTD and MTTR metrics into days and hours, and more ideally to minutes. The way to move the needle on these metrics is with Security Intelligence.

Security Intelligence isn't derived from a single technology but from a tightly integrated group of technologies that provide the required forensic visibility and that work together to help security teams most efficiently discover, qualify, investigate, mitigate and recover from threats.

A unified approach to Security Intelligence ensures that technology, people and processes are precisely aligned towards the objective of reducing MTTD and MTTR—and ultimately, to reducing business risk.

How to Gauge an Organization's Security Intelligence Maturity

Executive leaders want to know where their organizations fall on the spectrum of capabilities to reduce risk attributed to security threats. The LogRhythm Security Intelligence Maturity Model™ (SIMM™) helps companies understand their business risk posture based on their Security Intelligence capabilities and organizational characteristics. The levels of maturity span from Level 0, where a company has not invested in Security Intelligence capabilities at all, and is therefore at high risk of successful cyber attacks; to Level 1, which addresses minimal compliance related requirements; to Level 2, in which the company has an efficient compliance posture and is gaining visibility with improved capabilities to respond to threats; to Level 3, in which the company is vigilant in seeing and quickly responding to most threats; and finally to Level 4, in which a company is capable of withstanding and defending against the most extreme attacks from determined adversaries.

(View an Executive Summary of the Security Intelligence Maturity Model in Appendix A.)

Executive leaders want to know where their organizations fall on the spectrum of capabilities to reduce risk attributed to security threats.

Astute organizations attempt to move up the scale of the SIMM in order to build a resilient security posture that can fend off attacks with the potential to damage the company. Upward movement on the maturity model is dependent upon detection and response capabilities underpinned by security technologies such as holistic log management, network and endpoint forensics, behavioral and correlative analytics, security information and event management (SIEM), and more.

Full maturity on the SIMM means that an organization:

- Has an extremely resilient and highly efficient regulatory compliance posture
- Is able to see and quickly respond to all classes of cyber threats
- Is able to see evidence of the most insidious kinds of threats (such as advanced persistent threats, or APTs) early in their lifecycle and is able to mitigate their activities
- Can withstand and defend against the most extreme nation-state level adversary

As organizations evolve their Security Intelligence maturity, the realized reduction in MTTD and MTTR significantly reduces the risk of experiencing a damaging cyber incident. Of course, each organization needs to assess for itself the appropriate level of maturity it seeks to attain based on its own risk tolerances.

Fortunately, organizations with limited budget and higher risk tolerances can achieve significant improvements in capability by moving towards a Level 2 posture. For organizations with more cyber security resources and much lower risk tolerances, targeting Level 3 or even 4 might be appropriate.

LogRhythm's unified platform approach and flexible product architecture allow an organization to adopt and mature capabilities over time, comfortable in the fact that subsequent investments will build on previous steps along the maturity model. LogRhythm's goal is to ensure that enterprises have a partner able to provide the integrated technology building blocks, and associated services, to most effectively and efficiently empower those enterprises to realize their Security Intelligence objectives and best protect themselves from damaging cyber threats.

Conclusion

Corporate CEOs and Board members have a fiduciary responsibility to know and understand their organization's IT security and business risk posture; i.e., where the company sits on the Security Intelligence Maturity Model. They must weigh the organization's appetite for risk with the current capabilities to mitigate it, and then make a plan to close the gap if one exists. The LogRhythm Security Intelligence Maturity Model is a valuable guide for building the necessary successive layers of threat detection and response capabilities.

About LogRhythm

LogRhythm, the leader in security intelligence and analytics, empowers organizations around the globe to rapidly detect, respond to and neutralize damaging cyber threats. The company's patented and award-winning platform uniquely unifies next-generation SIEM, log management, network and endpoint forensics, and advanced security analytics. In addition to protecting customers from the risks associated with cyber threats, LogRhythm provides unparalleled compliance automation and assurance, and enhanced IT intelligence.

LogRhythm is consistently recognized as a market leader. The company has been positioned as a Leader in Gartner's SIEM Magic Quadrant report for three consecutive years, named a "Champion" in Info-Tech Research Group's 2014-15 SIEM Vendor Landscape report and ranked Best-in-Class (No. 1) in DCIG's 2014-15 SIEM Appliance Buyer's Guide. In addition, LogRhythm has received Frost & Sullivan's SIEM Global Market Penetration Leadership Award and been named a Top Workplace by the Denver Post.

To download or forward the complement to this paper, **Surfacing Critical Cyber Threats Through Security Intelligence: *A Reference Model for IT Security Practitioners***, go to: www.logrhythm.com/SIMM-CISO.

Appendix A

Executive Summary of the LogRhythm Security Intelligence Maturity Model

Organizational Security Intelligence capabilities by maturity level are summarized in the chart below.

CAPABILITY	DESCRIPTION	LEVEL 0	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4
	MTTD TYPICALLY MEASURED IN:	2015 YEARS	MONTHS	DAYS	HOURS	MINUTES
	MTTR TYPICALLY MEASURED IN:	MONTHS	WEEKS	DAYS	HOURS	MINUTES
SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)	The organization has deployed a SIEM and is leveraging dashboards, analysis, reporting, risk management, alerting, and incident response orchestration and automation capabilities.	○	◔	◑	◕	●
LOG MANAGEMENT	The organization has deployed a standard Log Management solution providing centralized and secure acquisition of forensic log, machine, and event data.	○	◔	◕	●	●
SERVER FORENSICS	The organization has deployed Agents to Servers providing deep forensic level visibility into server activity including file integrity monitoring, registry monitoring, process activity monitoring, network activity monitoring, and more.	○	◔	◕	●	●
ENDPOINT FORENSICS	The organization has deployed Agents to Endpoints providing deep forensic level visibility into workstation and mobile device activity including file integrity monitoring, registry monitoring, process activity monitoring, network activity monitoring, and more.	○	○	○	◑	●
NETWORK FORENSICS	The organization has Network Forensic sensors for monitoring internal and external network traffic activity, including full packet capture.	○	○	○	◑	●
MACHINE ANALYTICS	The organization has deployed real-time, automated analytics technology that can leverage all log data, environmental context and intelligence to identify and prioritize threats via a variety of analytics approaches such as advanced correlation and behavioral anomaly detection.	○	○	◑	◕	●
VULNERABILITY INTELLIGENCE	The organization is actively scanning and assessing the environment for vulnerabilities that could be leveraged by a threat actor and leveraging this intelligence in support of improved analytics and overall security posture.	○	○	◔	◕	●
THREAT INTELLIGENCE	The organization is leveraging open source, community, and commercial threat intelligence, across various threat vectors, in support of improved analytics and overall security posture.	○	○	◔	◕	●
MONITORING AND RESPONSE PROCESSES	The organization has developed standard processes and procedures for monitoring and responding to threats and any associated incidents.	○	◔	◑	●	●
SECURITY OPERATIONS CENTER	The organization has implemented a Security Operations Center able to provide 24/7 "eyes on the glass" and provide global orchestration and implementation of threat analysis and incident response.	○	○	○	◑	●

Continued on page 10

Appendix A

Executive Summary of the LogRhythm Security Intelligence Maturity Model *continued*

Organizational risk characteristics by maturity level are summarized in the chart below.

RISK CHARACTERISTIC	DESCRIPTION	LEVEL 0	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4
COMPLIANCE RISK	The organization is able to comfortably and efficiently meet all mandated compliance requirements.	○	◑	●	●	●
INSIDER THREAT RISK	The organization is able to detect and respond to most threats originating from, or acting within, the internal protected environment.	○	◔	◑	●	●
EXTERNAL THREAT RISK	The organization is able to detect and respond to most threats originating from outside the protected environment.	○	◔	◕	●	●
ADVANCED PERSISTENT THREAT (APT) RISK	The organization is able to detect, respond, and defend itself from threats leveraging APT type capabilities in support of criminal, activist, terrorist, or espionage related objectives.	○	○	◔	◕	●
NATION STATE THREAT RISK	The organization is able to detect, respond, and defend itself against a highly motivated nation state level adversary.	○	○	○	◑	●

LogRhythm™
The Security Intelligence Company

LR_SIMM_CEO_01.15

LogRhythm™