Best Practices for Corporate Cyberintelligence Processes

Cyberincident response is no different than any other type of warfare. It requires strategy, tactics, planning, technology, psychology and intelligence. Furthermore, history repeatedly demonstrates that numerically inferior forces that are armed with less capable technologies can win when generals are armed with accurate intelligence. As the Chinese military strategist Sun Tzu wrote in *The Art of War*, "The reason the enlightened prince and the wise general conquer the enemy whenever they move and their achievements surpass those of ordinary men is foreknowledge."[1]

For those who have ever had the inimitable honor of executing incident response in cybersecurity, the feeling of being an underdog is likely familiar. Using a proactive approach including intelligence-based processes and mitigation plans is highly recommended. This article offers a framework for those who seek to leverage security posture by implementing cyberintelligence processes in information security programs. This framework reflects military experience and is based on three subdisciplines in *The Art of War*: the strategic, operational and tactical levels.[2] Leveraging methodology with accessibility, this article combines recommended intelligence processes and examples from on-the-job experience.

Cyberintelligence Processes on the Strategic Level

These days, consolidating intelligence into C-suite decision-making processes should be standard. In this regard, intelligence-based decision-making is a proper process in the information security realm. Moreover, if a corporation must conform to sectorial regulations or well-known standards, the firm will also likely be obligated to perform certain intelligence processes. One way or another, chief information security officers (CISOs) should take initiative and incorporate intelligence into their reports to the board.

Cybersecurity Threat Landscape

Many information security companies tend to publish annual and seasonal threat landscape reports. The CISO should use this vital information to implement risk assessments while developing annual work plans and long-term security roadmaps. This is especially crucial for designing and developing cybersecurity force structures and capabilities in an organization. For instance, statistics show that 91 percent of cyberattacks start with a phishing email as the delivery vector.[3] This information should lead an organization to decide to review its relevant controls and to consider upgrading related security systems, e.g., mail protection and sandbox. In mid-2014, and even more so in 2015, ransomware campaign outbreaks became more prevalent.[4] When these issues arose, organizations should have sought to secure their networks, properly assemble situational evaluations and develop dedicated mitigation plans to combine prevention tools, incident response, storage backup, etc. Phishing emails and past ransomware outbreaks should have been game changers for

Ofir Eitan, CISM
Is a cybersecurity manager at Leumi Card, the second largest payment company in Israel. He was formerly head of the Israel National Cyber Bureau Situation Room and acting head of the CERT-IL (Israel's Computer Emergency Response Team) Hotline. Prior to that, Eitan served in the Israeli Intelligence Corps in various positions as an information security officer and cyberthreat intelligence (CTI) team leader.

Aviv Srour
Is a cybersecurity expert, currently working as CTI team leader at White-Hat Ltd. Formerly, Srour was an incident response analyst at Leumi Card and a cybersecurity incident response team (CIRT) leader in the Israeli Air Force. In his positions, Srour demonstrates a strong background in the fields of cyberintelligence, computer forensics and incident response.

most organizations, but if an enterprise still has not been a victim two or three years later, it is just luck, and prevention plans should still be developed.

Periodic Intelligence Board Briefing

The presentation of a business case plays a large role in the information security industry, and intelligence is a very beneficial tool for CISOs to explain their agendas. Executives tend to show interest in intelligence reports, so the CISO should deliver consistent, mandatory cyberintelligence presentations to the board of directors. This gives the CISO a direct line to deliver relevant agendas to the C-suite. A CISO can even use case studies and trends to back up the agenda and business cases with actionable information and business impact analysis.

> “EXECUTIVES TEND TO SHOW INTEREST IN INTELLIGENCE REPORTS, SO THE CISO SHOULD DELIVER CONSISTENT, MANDATORY CYBERINTELLIGENCE PRESENTATIONS TO THE BOARD OF DIRECTORS.”

Cyberintelligence Processes at the Operational Level

Intelligence has a large role in national security, military affairs and business between corporations. In a volatile, uncertain, complex and ambiguous (VUCA) environment where “fog of war” spreads everywhere and information overflows, the decision-making process is challenging. Because of this, large organizations use intelligence to ease the complexity of this challenge and to perform risk assessments more accurately and relevantly. The same applies to cyber security; therefore, it is highly recommended that an organization combines intelligence into decision-making processes.

Intelligence-Based Incident Response Decision Making

The following example illustrates a proper process. In 2016, one of Israel’s leading organizations had technical difficulties with their customer relationship management (CRM) system. Simultaneously, many organizations were facing ransomware outbreaks. During this time, the local security community received many alerts from various sources, including the national Computer Emergency Response Team (CERT), cyberintelligence vendors and information security service providers. The organization’s service organization control (SOC) was put on high alert and started to increase monitoring processes. It was discovered shortly after that the antivirus blocked an early version of the ransomware. Additionally, the organization’s intrusion prevention system (IPS) blocked a command and control (C&C) connection attempt by the TeslaCrypt ransomware. This was due to a successful implementation of an indicator of compromise (IOC) list sent by an intelligence vendor a week prior. After a short evaluation of the situation, the information security unit instructed the IT department to immediately carry out a patch management process based on a common vulnerabilities and exposures (CVE) list to patch the exploits of the related ransomware.

The interesting part of this case was the fact that the IT department was facing a lack of available human resources, and the available resources were busy trying to solve the CRM problem. Moreover, according to procedures, at least one week of test performances is needed before running

patches on production servers. Now, the company faced a dilemma. On one hand, security issues had increased drastically, and on the other hand, business continuity should be a priority. After an IS and IT joint meeting, it was decided to boost efforts to solve the CRM problem and, once finished, to divert the resources back-to-back to carry out an expedited testing procedure of the patch management process. Meanwhile, as a first layer of defense, the IS unit was in charge of implementing online IOC lists directly to the security systems.

Intelligence-Based Mitigation Planning

New cyberattack tools, methods and vectors are constantly evolving and changing. Best practices and security technologies are respectively behind as a result. For this reason, information security managers are advised to combine new intelligence information when developing security mitigation plans and programs and updating procedures. Moreover, information security projects should be prioritized based on the current threat landscape.

The following organizational example illustrates intelligence-based mitigation planning. An organization conducted a review at the beginning of 2016 to examine its ability to contain ransomware attacks, based on intelligence analysis. The project spanned a quarter and was presented to the chief information officer (CIO) and the senior IT managers once completed. The report included:

- **Intelligence briefing**—Threat evolution, kill chain, case studies and risk assessment with regard to the threat of ransomwares
- **Best practice**—Based on an analysis of various articles, due to lack of formal references and frameworks focused on mitigating risk posed by ransomware
- **Internal review**—Of the current controls, procedures and recovery capabilities relating to the offered best practice
- **Conclusion**—Risk evaluation, business impact analysis and a suggested information security plan

This project accomplished a variety of goals. First, it raised the attention and awareness of senior IT managers and executives. Second, and no less important, different IT and business units in the organization were able to come together to analyze risk and develop solutions to reduce it. For instance, a meeting with the head of storage established a true, deep understanding of the organization's ability to recover from a ransomware attack. Third, it was determined that some of the security system implementation plans needed a second review, mainly for changing policy and hardening configurations (e.g., the email security gateway). And finally, information security plans for the following year were designed according to project results and findings. For example, a dedicated readiness program was executed and applied to different ransomware attack scenarios. Also, cyberrisk maps were updated and the organization incident response plan was validated.

Cyberintelligence Processes on the Tactical Level

Tactical intelligence processes reflect daily activities that need to be carried out by incident responders, security analysts and SOC practitioners. The suggested framework is based on the core process of adequate implementation of IOC into security systems. An IOC refers to artifacts that indicate a malware footprint probability in an IT network, e.g., C&C servers, CVEs, file names and registry keys.

> “IMPLEMENTING IOC FEEDS FROM MULTIPLE SOURCES THAT ALIGN WITH BUSINESS OBJECTIVES IS RECOMMENDED.”

Source mapping is the first step to malicious activity monitoring using IOC. One can reasonably assume that if the organization forms medium to high maturity level incident response processes, the practice of source mapping would be obtained differently. In general, IOC feeds can be found in four different ways:

1. Free via the Internet
2. Open or direct from government agencies—such as a national CERT or regulator
3. Shared alerts in information security communities on social networks and institutions
4. And, as expected, for sale by vendors

Implementing IOC feeds from multiple sources that align with business objectives is recommended. Additionally, developing and maintaining a private IOC warehouse, which should contain relevant threats and form automation for the network security systems and appliances (such as IPS or endpoint detection and response [EDR]), is highly advised. Common information security risk management and incident response methodologies suggest conducting tactical cyberintelligence processes using the following three security approaches: prevention, detection and response.

Prevention

Conducting prevention procedures is a smart, cost-effective approach to address threats. Usually, it requires little effort and mitigates potential threats well. To create and implement the following processes and to stay ahead of current campaigns and malware spreads, the following are recommended:

- **IOC blocking**—Daily base blocking of Internet protocols (IPs), domains, hashes, mail addresses, etc. Note that blocking the wrong IP could be devastating for the organization, so examine sources thoroughly and create automated processes for highly reliable feeds. This kind of automation can save the organization lots of time, since it will not need to manually feed security products with malicious IOCs.
- **Patching**—Patch management is the most cost-effective way to prevent advanced cyberthreats. If a high-severity exploit exists and uses a specific vulnerability in the enterprise system, patch it right away. If this seems like overkill, consider the WannaCry attack. It is well known in the worldwide cybersecurity community that the patch to the WannaCry exploit was released a few weeks before the ransomware outbreak.

- **Configuration changes**—For certain malware attacks, a list of IOC and CVEs may not yet exist; however, the severity level and the business impact in the case of a compromise are critical. In this case, configuration changes can be implemented as a temporary control until a validated patch or other security countermeasure can be put in place. For example, during the WannaCry ransomware outbreak in May 2017, security researchers advised blocking Server Message Block (SMB) v.1 protocol across the network to prevent malware from spreading.

Detection

This process focuses on implementing IOCs into security information and event management (SIEM) for an efficient analysis of events and to create new alerts based on intelligence rules. The detection process has become an inherent countermeasure for any SOC team due to the need for a massive reduction in false positives and as a cost-benefit solution for event floods. The process has become much easier as of late because security systems have started supporting open application programming interface (API). Therefore, one can create automatic scripts to implement IOCs automatically. For more information about IOC automation, read about popular protocols for IOC exchange such as structured threat information expression (STIX) and Open IOC. On that note, one major question to address is which indicators to block and which to monitor. As mentioned previously, the main consideration should address the source. Furthermore, the strength of the artifact should be taken into consideration. For example, hash, unique registry key and malicious URLs will cause fewer false positives than IP, which can change much more rapidly due to evasion techniques used by the adversary, making it a weaker indicator.

> “AI IS BASED ON THE ASSUMPTION THAT AN ADVANCED CYBERATTACKER WOULD LEAVE FOOTPRINTS IN A COMPROMISED NETWORK EVEN IF A FULL IOC LIST IS NOT AVAILABLE.”

Another process that should be taken into consideration is the combination of artificial intelligence (AI) as an integral technology in cybersecurity alignment. AI techniques can improve overall security performance where conventional security systems can be slow and unsatisfactory. They can provide better protection against the increasing number of sophisticated cyberthreats. In some cases, a list of IOCs is not enough or only partially exists due to insufficient analysis. AI is based on the assumption that an advanced cyberattacker would leave footprints in a compromised network even if a full IOC list is not available. According to the AI paradigm, IOCs are considered traditional systems, since they rely on predictable templates and algorithms. Therefore, AI offers a solution to this issue by upgrading the organization's intrusion detection and prevention system (IDPS) to the next level—a level where anomaly patterns are not implemented as a feed (from a cloud or by installation) but can detect new threats and produce intelligence information by comparing and analyzing network traffic to a baseline analysis before a compromise occurs.

Response

Consider the example of a SOC analyst calling to report irregular traffic observed from the CIO's computer at an unknown IP address. The analyst is waiting for instructions. What is the next step? Block the traffic and call it a day? Use forensics to analyze the source causing the traffic?

Now, what if the analyst mentioned the IP address was connected to Carbanak, one of the biggest Russian cybercrime groups? This piece of information is vital for analyzing the alert and could be a game changer for decision-making in an incident response process. Although blocking the IP address for outbound connection from the organization's network might sound like the best first step to take, some questions should be considered before one chooses the best mitigation or remediation step:

- Is the IP address (or any other artifact) still used by the attacker?
- Is there a URL attached to this IP address that can be blocked?
- Would blocking connection to this IP (or any other artifact in use) disrupt business delivery?
- If the answer to one of the previous questions is yes, is there a better alternative remediation action to execute?

Due to the fact that corporations all over the world are under threat of being compromised by adversaries on a daily basis, cybersecurity is no different than a military campaign. Therefore, it requires conduct of operations in addition to force design and force structure processes. In terms of managing cybersecurity, these disciplines respectively resemble incident response and cyberreadiness. For this reason, cyberintelligence plays a vital role in increasing the organization security posture by supporting major processes in all spheres whether it is on a strategic level (by designing the information security roadmap and presenting it to the board), on an operational level (by assisting planning mitigation plans and programs) or on a tactical level (by supporting incident response by delivering IOC for cyberoperations).

Endnotes

1 Tzu, S.; *The Art of War*, translated by S. Griffith, Oxford University Press, USA and England, 1964

2 *Ibid*.

3 Zurier, S.; "91% of Cyberattacks Start With a Phishing Email," *Dark Reading*, 13 December 2016, *www.darkreading.com/endpoint/91--of-cyberattacks-start-with-a-phishing-email/d/d-id/1327704*

4 Hughes, M.; "From Russia With Hate," MakeUseOf.com, 26 July 2016, *www.makeuseof.com/tag/history-ransomware-russia-reveton/*