Managing Risk to Reduce the Impact of a Breach

In today's information security environment, organizations are moving beyond simply lowering the probability of a breach to limiting the impact if a breach occurs.

Rapid detection and effective response are now clearly in focus, and organizations are spending time and money to manage growing security responsibilities which now include: operating a monitoring infrastructure, investigating alerts, and responding to incidents. Without this investment, organizations risk missing requirements necessary for regulatory compliance and the warning signs of incidents while they are in progress.

In this paper, we review the targets that organizations should set to achieve adequate detection and response.

Introduction

Today's CISO must participate in risk management conversations with the C-Suite and the Board of Directors. Organizations now plan for cyber threats as foreseeable events that lead to expensive data breaches, disruption to operations, and outright theft. Additionally, regulators are compelling CIOs, CISOs, and CTOs to develop and manage KPIs that demonstrate management of this information security risk. As a result, leaders are managing information security risk analysis as they would any other business risk. As part of this strategic shift, organizations must also determine how to allocate budget to best address the growing information security risk and the regulatory requirements that come with it.

Assessing Information Security Risk

Building the case to invest in information security has not always been straightforward. We approach the cost of potential information security breaches with a relatively simple equation: $R = Pv * I$

R → Monetary risk for a company
P → Probability of a security incident
v → Vulnerability affecting the network
I → Impact of that security incident (usually expressed in dollars):

The dollar value of IT security risk is equal to the probability of an undesired outcome multiplied by the potential impact of that event. We know that, despite substantial investments in preventive controls, the combination of commoditized attack tools, organized crime as a successful business model, and emboldened nation-states makes the remaining risk of security incidents high enough to be meaningful. We also know that the cost impact of disclosure of protected records, theft, extortion, and/or disruption of critical services can be on the order of hundreds of millions.

With this knowledge, an increasing number of CISOs are shifting the Information Security conversation away from merely attempting to keep intruders out of the network. Instead, they are getting buy-in from the C-Suite by shifting the discussion to managing the impact of foreseeable risk-related cyber events[1]. To reduce the impact, rapid detection and response is required.

Reducing Risk to Your Organization

Today, risk management strategies structure the security program around an industry recognized framework, such as the HITRUST Cybersecurity Framework[2] or the federally established NIST Cybersecurity Framework[3]. Developing a framework that is attuned to the organization is a key step toward

understanding risk tolerance for foreseeable breaches. The NIST CSF specifically addresses five functions for a comprehensive security program: identify, prevent, detect, respond, and recover. Risk assessment and management are categorized under the identification function of the security program, which then informs the cascading requirements to fulfill the prevention, detection, and response functions.

Prevention

To reduce the probability of a security incident, the IT security organization builds a security perimeter and implements methods for preventing an attack. Organizations that have systems that connect to the internet, or allow their employees to access the internet, must take steps to prevent hacks. Mature organizations design a comprehensive security plan to prevent malicious attacks, and nearly all organizations invest in technologies that are designed to prevent network and system incursions.

In general, organizations use a combination of the following technologies to resist attempts to compromise organizational assets:

- Firewalls, routers, and switches
- Intrusion Prevention Systems
- Application Firewalls
- Email and URL filtering
- Vulnerability Management
- Anti-Virus/Endpoint Protection Products (AV/EPP)
- Patch Management
- Data Loss Prevention (DLP)
- Deception

Each of these technologies also produce activity logs and alert messages, which convey the frequency (and potentially the severity) of those attempts.

Detection and Response

The other factor in the risk equation is the impact of an attack. The best way for an organization to reduce this variable is to improve both their ability to detect when an attacker has breached the network and also the organization's speed to full remediation and recovery.

When security professionals think about how to minimize the impact of a compromise, they should focus on minimizing two metrics, which together constitute the "Dwell Time":

1. The time from initial compromise to detection
2. The time to reach full recovery after detection

Dwell time is observed to average up to 200 days[4] in reported breaches.

In detecting compromises, there are many ways that a company can gather data that will help identify events worth investigating:

- Intrusion Detection Systems (IDS)
- Full Network Packet Capture
- Netflow Data (Packet Metadata)
- Logs from on-premise and SaaS applications
- Logs and alerts from preventive and other security technologies
- Security Information and Event Management (SIEM)

The preventive controls detailed in the prior section also create early warning messaging, which can be considered valuable threat intelligence, in that they can identify 'doorknob-twisting' that precedes actual penetration and compromise.

With first level detection in place, the organization then invests in humans and technologies to investigate the multitude of events or alerts. See the section below on Alert Management.

Finally, the last item is a rapid, effective response capability. Incident response planning is a necessary part of a security program but is beyond the scope of this paper.

Together, detection and response can minimize the impact of an event, containing it, for example, to a single compromised workstation cleanup.

Alert Management

The multitude of data sources and detective technologies result in alerts of varying severity. To collect and evaluate the alerts, many organizations use SIEM systems to aggregate information from the data sources listed above, among various others. The SIEMs ingest all the data and trigger alerts for review as needed.

In reality, most alerts that security technologies generate do not indicate an actual compromised asset in the organization's environment. As a result, it is important for someone on the IT or Security team to evaluate each alert and then fully investigate the ones that appear to be genuine issues. In many sectors, there are stringent regulatory requirements that make investigation of security alerts mandatory, i.e. Health Insurance Portability and Accountability Act (HIPAA)[5] or the PCI Data Security Standard[6].

Options to Detect and Respond

When a company comes to the determination that their risk management strategy must include a robust detection and response capability, what is the best way to do so? In the next piece in our series, we explore four main strategies an organization can implement:

- Do nothing and accept the risk of breach.
- Assign security event review, investigation, and response tasks to existing IT staff.
- Build and staff an in-house security operations center (SOC) to manage the day-to-day elements of detection and response.
- Hire a trusted third party to provide the detection and response capabilities of a mature SOC.

You can see a detailed comparison of these four options, including benefits and costs, in our paper, "Detection & Response: 4 Options for Security Operations."

Endnotes

[1] "Foreseeable Risk", Dictionary.com, https://dictionary.law.com/Default.aspx?selected=770

[2] "Understanding and Leveraging the CSF," HITRUST, February 2018, https://hitrustalliance.net/understanding-leveraging-csf/

[3] "NIST Cybersecurity Framework," National Institute of Standards and Technology, https://www.nist.gov/cyberframework

[4] "2018 Cost of a Data Breach Study: Global Overview," Ponemon Institute, https://www.ibm.com/security/data-breach/

[5] "Summary of the HIPAA Security Rule," Office for Civil Rights, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

[6] "PCI Security," PCI Security Standards Council, https://www.pcisecuritystandards.org/pci_security/