Secureworks®

WHITE PAPER

Insider Attacks: Protecting Your Business From Itself

For organizations trying to proactively manage their cybersecurity operations, there is a multitude of threats to consider. You're constantly hearing about the evolving threat landscape and trying to keep tabs on malicious threat actors, but what about the possible threats originating within your company? According to a Ponemon Institute study, the number of insider security incidents has increased by 47% since 2018. Further, the average annual cost of these threats has grown by 31% to $11.45 million.[1]

47%

increase in insider security incidents since 2018.

31%

increase of average annual cost of threats to $11.45 million.

Despite these statistics, insider threats are easy to overlook given the emphasis put on external threat actors, but they should still be given consideration when evaluating your cyber risk and addressing your security strategy.

Motives and Organizational Awareness

Diagnosing insider threats comes down to a person's intentions, and motivations can vary from sabotage and espionage to personal benefit, or even attempts to ruin a company's reputation. Some individuals wish to obtain intellectual property (IP) or critical confidential information – a unique chemical formula or a client list, for example – for financial gain or to start their own company. Or disgruntled departing employees may want to inflict harm on their soon-to-be former employer. More often than not, however, insider incidents are caused by negligent employees or contractors. Far less common, but still plausible, are hires strategically placed into companies by nation-state threat actors. While incidents involving criminal insiders are not widespread, their potential cost to an organization still warrants attention.[2]

There is a wide range of security risk among organizations, dependent upon several factors including industry and size. A financial company that has thousands of employees, operates in dozens of locations globally, and has highly sensitive or valuable IP to protect is inherently more at risk than a local retailer that may have an online presence but doesn't collect as much private customer data. The degree of awareness and preparedness to prevent insider attacks often has a direct correlation to an organization's risk profile. More employees translate to more endpoints to secure, and having valuable IP means more data to protect. Large organizations with more than 75,000 employees spent an average of $17.92 million responding to insider threat incidents, in contrast to organizations with a headcount below 500 spending $7.68 million on average.[3] However, companies of all sizes and industries today have some cyber footprint and therefore should seek to implement adequate security measures.

[1] Ponemon Institute, The Real Cost of Insider Threats in 2020
[2] Ponemon Institute, The Real Cost of Insider Threats in 2020
[3] Ponemon Institute, The Real Cost of Insider Threats in 2020

Steps to Remediate

Let's say you've experienced the misfortune of discovering a breach originating from inside your business. How should you respond? In the aftermath of an insider attack, this checklist, while not exhaustive, can serve as a resource to help guide your response.

1. Consult with general counsel

Any action you take should be done with sound legal advice. Maintain a close relationship with your general counsel or an outside firm during every step of your response plan to ensure compliance with applicable laws and regulations.

2. Reference your plan

In the aftermath of a breach, the natural inclination is to react quickly. In these instances, it's important to take a step back and consider a measured approach to what you want to do (or in some cases, not do). Ideally, an incident response (IR) plan should already exist, and you should be able to reference it for guidance. This plan should include everything from employee communication to your PR strategy. Collaborate with cross-functional stakeholders to implement the steps outlined by the plan.

3. Conduct an investigation

Any breach requires a thorough investigation to map out exactly what happened. In the case of an insider attack, it's critical to understand what artifacts you have that may demonstrate the loss of IP. Identify and retrieve the devices the offending individual used or had access to and find out what state they are in. Preserving devices may not be possible during an IR situation; however, preservation may be valuable if the case will involve a legal proceeding or regulatory actions.

4. Seek guidance from Human Resources (HR), Labor Unions, or Works Councils

As with any personnel issue, your HR department or whatever body represents your employees should be involved in the case of an insider attack to advise on the appropriate punitive response within policy guidelines. This group would also be able to speak to what remediation tactics or policies the offending employee may attempt to use in defense of their actions. Finally, HR may want to review the company's hiring process to ensure nothing was missed or overlooked in the vetting process that may have been a red flag to possible malicious behavior.

5. Do an inventory of your data

Understanding what types of data you have (e.g., HR, financial, IP), what regulations govern the data (e.g., GDPR, CCPA), where you store it, what systems can access it, and what individuals have access to those systems is a required process for any organization. Ideally, an inventory should be done regularly – not only in reaction to an incident – to ensure necessary security controls are in place to protect your assets.

6. Conduct a "lessons learned" exercise

Learning from an insider attack is a good way to prevent one from happening in the future. Sit down with the key players involved in the incident to find out what led to the breach and identify factors that helped or inhibited the investigation. An independent third-party security vendor with an IR function can help facilitate this process.

7. Evaluate your risk management program

Prevention starts with an organization's evaluation and awareness of its environment and risk profile. Work with your organization's risk management function to determine what security controls you have in place. What data loss prevention (DLP) or privileged access management (PAM) tools are you using? Have you considered a security analytics platform that uses AI to detect behavioral anomalies? These are just a few questions to ask as you evaluate your risk management strategy and take steps toward prevention.

The unfortunate reality is that many organizations have a reactive and incident-driven security program.[4] Companies that may have previously taken a "check the box" approach to security would benefit from a comprehensive review of their systems. A key question that may arise in this review is: Do you have a security partner, and if so, is that provider equipped to help you mitigate the risks your organization faces? Assessing your current security architecture – including considering a vendor or changing from an existing vendor – can also help you improve your overall security posture. With a wide array of security providers available, it's important to identify your needs and gaps to find the best match for your organization. Following steps 6 and 7 outlined above will help you get there. Partnering with an experienced security provider can provide expertise, resources, and proactive incident response solutions to ensure you're prepared for what's ahead.

The Role of Culture in Prevention

From the start, staff should understand their role and responsibility related to organizational security. Educating employees after an attack occurs is too late. All employees, beyond just IT, should understand the responsibility of their access and the ramifications should a breach occur. Establishing a culture of security mindfulness pays great dividends to an organization across the board. When everyone understands the role they play in keeping their company secure, the whole company benefits. This awareness plays a role in prevention, as employees may be more likely to report suspicious behavior if they know what to look out for.

Preventing insider threats should be part of a holistic security program. No matter where or how a cyberattack originates, knowing and constantly evaluating your organizational risk is the most important step to prevention.

Preventing insider threats should be part of a holistic security program. No matter where or how a cyberattack originates, knowing and constantly evaluating your organizational risk is the most important step to prevention.

[4] Ponemon Institute, The Cybersecurity Illusion: Enterprise Security Remains Reactive

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp