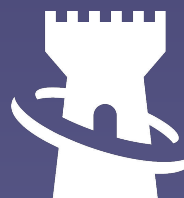




Is Your
**Greatest
Cyber Risk**
Hiding in
Plain Sight?

How to Combat Insider Threat

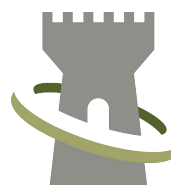


SECURE HALO
SECURING THE ENTERPRISE

Leading Threat Vector — Insiders

The first thought when it comes to securing the enterprise in today's increasingly connected world is likely to revolve around external components like firewalls and anti-virus software. While these are necessary elements of the overall security process, they fail to take into consideration what continues to be the greatest cyber risk to any organization — insider threat.

A whopping 77 percent of internal breaches were deemed to be by employees, compared to just 11 percent by external actors only, according to the [Verizon 2016 Data Breach Investigations Report](#). Failing to account for a vulnerability of this size creates tremendous risk for all organizations, regardless of the hardware and software that they have in place to mitigate threats.



SECURE HALO

SECURING THE ENTERPRISE


People: Your Greatest Asset and Weakest Link

Employees are the backbone of most organizations, yet their access to sensitive information and assets also makes them an inherent risk vector. Even if your organization already has security measures in place, do they consider internal actors or is the protection only outward facing? Do they account for employees who use their own mobile devices for work-related activities? Is there protocol for when traveling and using alternate networks/computers to access organizational data? Today's connected world means more opportunities for employees to act negligently when it comes to security, creating increased risks and vulnerabilities for your organization.

It's an oft-repeated yet true statement that the weakest link in a security chain is people. That's why it is imperative that organizations consider "people-centric" security practices, like understanding emerging threat trends that target individuals, the role that company culture plays in security, and the mindset of the average employee. Before diving into this critical issue, it is first necessary to understand exactly what insider threat is and its various types.

Insider threat is a current or former employee, contractor or someone who has or previously had authorized access to sensitive data, systems, technology, personnel, or other items of interest. In other words, basically anyone involved with your organization who can knowingly or unknowingly provide access to hackers or steal valuable information.


1 in 5 
will sell their work password for money

59% 
will steal proprietary corporate data when they quit or are fired

62% 
of employees involved in insider attacks are looking to establish a second stream of income off of employers' sensitive data

77% 
of internal breaches are conducted by employees and nearly 32% of all organizations have no capability to prevent insider threat

Source: Dark Reading | Fortune | Verizon Data Breach Investigations Report | Heimdal



“The risk associated with insider threat will continue to be ever present,” says Nick Streaker, Vice President of Technology for Secure Halo™.

“Organizations that have a proactive insider threat program focusing on the development and integration of insider threat controls, and monitoring across all of the organization’s business functions, from HR to IT, creates a defense in depth strategy that provides a solid foundation in preventing and mitigating the impact of the actions of an insider.”

Who is at Risk?

No organization is completely safe from insider threat. New technological security features won’t prevent an unaware and uneducated individual from clicking on a malicious link, or stop a motivated employee from stealing information.

For example, the 2016 hacking of Hillary Clinton campaign chairman John Podesta created prolonged damage to the Democratic party and generated international news coverage when Podesta clicked on a corrupt link in a phishing email written to look like it was sent by Google account management. In early 2017, a former National Security Agency (NSA) contractor was charged with stealing highly classified documents and storing them in his home and car over a period of several years. This occurred despite increased implementation of safeguards by the NSA following Edward Snowden’s infamous leak, demonstrating that truly any organization is vulnerable to insider threat.

Organizations should not take the approach that since they do not deal with proprietary information, they do not have to worry about insider threat. Intellectual property theft is not the only data at risk of compromise via insider threat. Employee information, like social security numbers, passwords to your network that staff members are willing to sell, or even access to your rolodex of clients are all additional areas that insider threat can breach. Knowing what to look for and being aware of warning signs can help prevent an insider attack from happening in the first place.

Recognize Insider Threat Profiles

Negligent Insiders—most of us, individuals who unwittingly allow access to company data. Whether this is through falling victim to a phishing campaign or via the use of public WiFi to view company information, these people unintentionally provide an opening for hackers to exploit.

Malicious Insiders—most often a disgruntled or departing employee, may knowingly steal or sabotage systems, intellectual property, or other important virtual or physical assets as a way of “getting back” at the organization for what they believe to be a wrongdoing. There are several other reasons driving the motivation to become a malicious insider, such as financial gain, the desire to be recognized or feel powerful, or to push their own political agenda.

Compromised Insiders—people who have had their credentials compromised or stolen by an outsider for purposes such as espionage, fraud, or attack. These individuals are likely to be susceptible to recruitment through social media or some other electronic medium like chat rooms or message boards, or could be acting as a response to blackmail, or out of loyalty to a colleague within the organization.

Connected Outsiders—A more connected world also creates organizations with larger digital ecosystems, which in turn leads to another type of insider threat. Third parties, vendors, or companies that make up your supply chain all have the potential for creating a back door into your system. Even with the proper security measures implemented and an educated staff in place, hackers can still break through defenses by exploiting a weak or nonexistent security system of a third party.

Each type of insider threat helps create the greatest cyber risk to your enterprise and is why considering it in a security plan is an absolute essential.

Insider Threat Warning Signs



Sudden behavioral changes: acting frustrated, vengeful, or unwilling to engage with colleagues



Unexplained affluence: could be payment for stolen data/passwords/ access to organization's network



Odd working hours: accessing the network outside of their normal business hours



Unusual movement of data: collecting information without a legitimate reason



Attempts to access unauthorized information: there's no need for this individual to be accessing this data, so why are they?



Violation of company policies: i.e. taking laptop home when policy is to leave it at the office

How Social Engineering Makes us all Potential Threats

Unfortunately, warning signs are usually specific just to malicious insiders, whereas the more common insider threat risk comes from the negligent insider. These individuals are often targeted through social engineering and do not realize they are being used to give hackers access to their system. This type of attack usually involves the following process:

Step 1

Hacker identifies info to create profile of target

Search for employment history, family data, hobbies, etc.

Step 2

Hacker builds relationship remotely using a cover that appeals to victim's preferences

Online connection invitation from a stranger; unsolicited job offer/interview

Step 3

Hacker gains access to your system

Malicious links, malware, resetting password

Step 4

Hacker infects entire organization's network

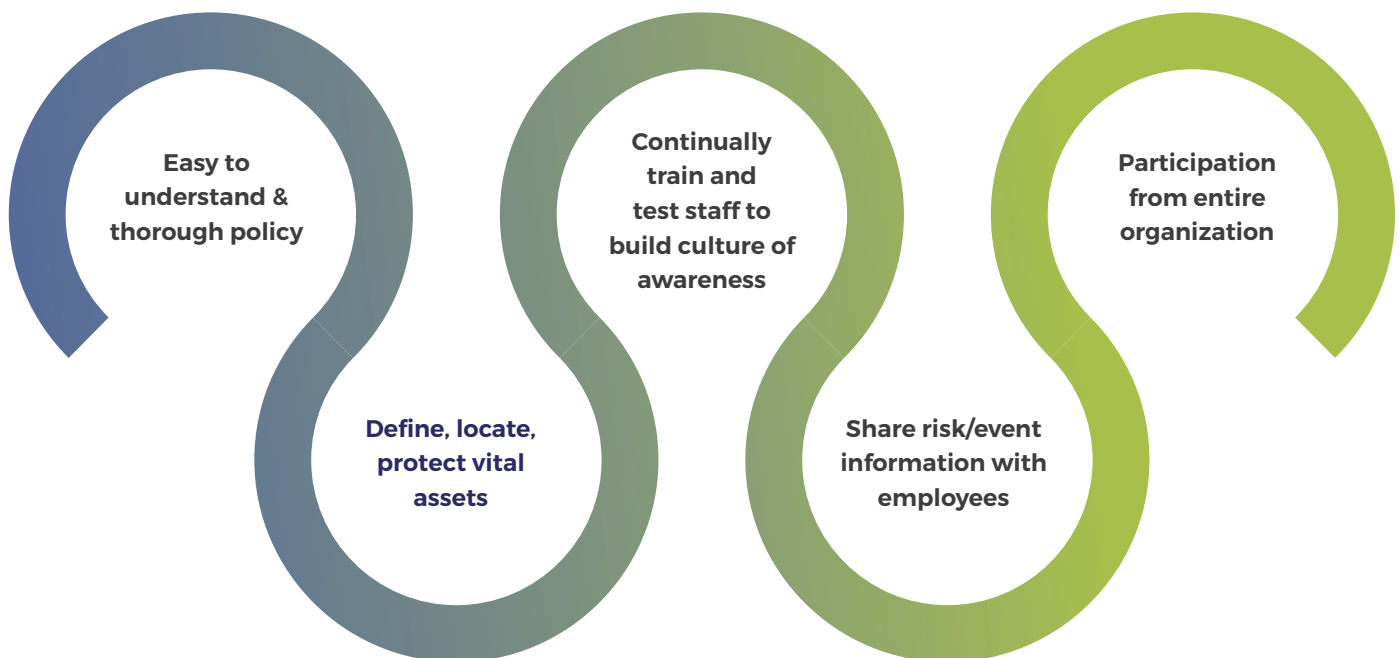
Once inside, the hacker can use the negligent insider to breach other systems unbeknownst to the victim

A specific form of social engineering called phishing or spear phishing is a popular method used during this process. This involves sending an individual a legitimate-looking email that contains an attachment or embedded link that delivers malware once opened or clicked. The victim is often unaware of any changes to their computer, despite having granted access to the hacker by downloading or clicking. Don't let the simplicity of this type of attack fool you. It's an effective way for hackers to gain access to entire networks and it can happen to anyone. This is why it is essential to develop a culture of cybersecurity awareness from the highest-ranking executives on down through the organizational chart.

Questions Boards and the C-Suite Should Ask About Insider Threat

Does our organization have an insider threat policy?

If not, one should be immediately created. If there is already a policy in place, it should be reviewed to ensure that it is both thorough and easy to understand for people in every department. The policy should be written in a way that employees of all security levels know exactly what to do and how to act, not just those involved in IT or security. Ensure that it is clearly stated that these requirements apply to everyone throughout the organization and that senior level staff is not exempt and will face the same repercussions for failing to adhere to the rules. Without participation throughout the entire organization, insider risks will remain as the biggest threat to your organization since you are only as strong as your weakest link.



Do we know what our “crown jewels” are and where they’re located?

An effective insider threat policy must take an organization’s critical assets into account. This includes identifying what your vital data and functions are so that business continuity can be maintained during a breach. Once identified, these assets must be explicitly located to minimize time wasted searching for them during an intrusion. Knowing exactly what and where your most important assets are will also help to better protect them.

What is our cybersecurity culture and what are we doing to promote it?

To foster a “culture of awareness,” provide real-life examples. Encourage employees to say something if they recognize a vulnerability or see something suspicious, like a fellow employee taking their work laptop home if organization policy is to keep it at the office. Set policies that require staff to verify changes or get authorization for wire transfers. Explain that organizational risk is directly tied to individual job security for employees to fully understand the importance of mitigating insider threat risk.

How are we ensuring that all outgoing and incoming activity is tracked and analyzed?

Performing internal audits and assessments is an ideal way to determine if employees are behaving in a manner that they should not be, like transferring sensitive information from one location to another. This process also includes assigning least privilege to users and programs so that an employee who doesn’t need access to organizational data in order to perform their job, is not given it. Even those with the highest level of access should still be monitored to ensure that sensitive information remains in the proper place.

What is the Human Resources department doing to reduce insider threat?

Threat mitigation begins during the hiring process. While detecting the negligent insider ahead of time is virtually impossible, determining the potential for a malicious insider is much more plausible. Falsified information on resumes or incorrect responses when asked about security situations could be potential warning signs. All new employees must be trained on the insider threat policy at your organization immediately upon being hired. Don’t limit training to only during onboarding or annual updates. This should be an ongoing process, with unscheduled testing of employees, so that insider threat remains in the minds of the entire staff.



Get Ahead of Insider Threat

An essential truth that is often ignored in the conversation about effective cybersecurity is that most theft within organizations is a result of a human being on the inside, either deliberately or inadvertently, and not the result of an external hacker. The latest software or hardware solutions can give a false sense of security since upwards of 75% of incidents involve some form of insider threat. So while technology is an important piece of the security picture, it's only one part of the larger picture.

Every organization has a capable detection team already in place—their employees. People are the first line of defense, so empower them to both detect and mitigate employee issues, which will help reduce insider threat risk, whether the threat is intentional or not.

Often, a cybersecurity approach is developed after an incident has already damaged an organization's value, innovation, or reputation. By then, it's too late. Instead, we encourage organizations to take a proactive approach: understand what data is at stake, establish policy and procedures, and educate and empower employees. This will help you get ahead of insider threat.

How Secure Halo™ Can Help

Companies need meaningful insight into how vulnerable they are to expanding and evolving digital risks, like insider threat. Secure Halo™ provides enterprise cyber risk assessments, managed services, and cybersecurity consulting to Fortune 500 companies and federal agencies. Our **Secure Halo™** platform provides a holistic view of cyber risk to empower market-driven and threat-based decisions, while also meeting regulatory requirements.

Learn more at www.securehalo.com