The Danger Within:
Unmasking Insider Threats

CYBERARK®

Contents

Introduction

"Insider Threat" has become a favorite industry buzzword, stemming largely from the massive data breach perpetuated by former U.S. National Security Agency (NSA) contractor Edward Snowden. Yet the majority of insider threats are far less conspicuous, won't make headlines and are not carried out intentionally—but they can cause crippling damage to an enterprise. To effectively protect against insider threats, organizations must first understand what the insider threat is. This eBook outlines the who, what, why and how of the insider threat to expose risks you may not be considering, and provides guidance to help you prevent and detect these costly attacks.

Overcoming Misconceptions: *Who* is the Insider Threat?

While many organizations have recognized this "threat from within" and bolstered protections accordingly, efforts typically focus on malicious insiders. However, a recent survey[1] of Information Security Forum (ISF) members shows that the vast majority of insider breaches were caused by inadvertent employee behavior; not by malicious users. To effectively protect against the insider threat, you must first understand who the insiders are. Insider threat actors can be categorized into four main groups: Exploited Insiders, External Insiders, Malicious Insiders and Unintentional Insiders.

69%

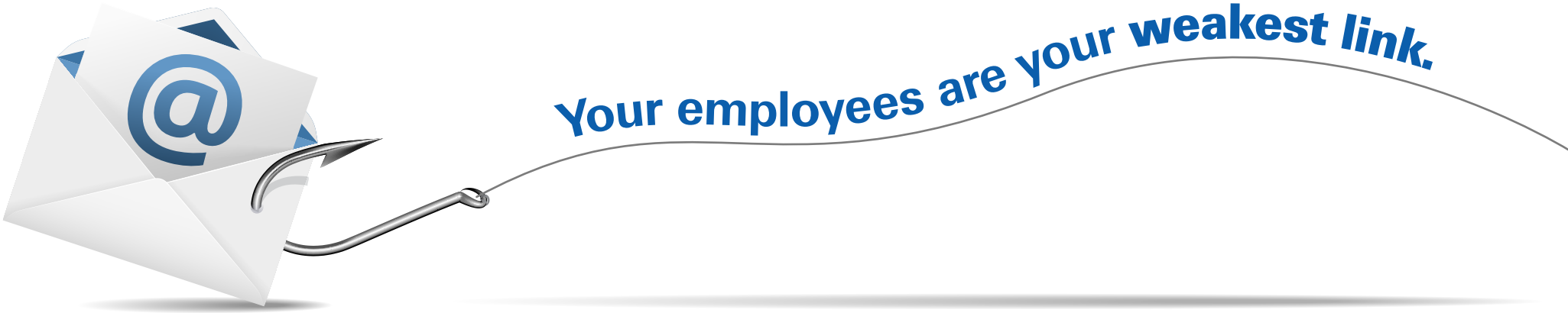
of organizations reported that they experienced attempted or successful data theft or corruption by corporate insiders during the prior 12 months.[2]

The Exploited Insider

Attackers commonly target high-value employees—such as sysadmins, IT help desk teams and executives—with spear phishing emails, and it only takes one victim for an attacker to establish a foothold inside the organization. Once inside a high-value user's machine, attackers can capture their privileged credentials, further escalate privileges, execute pass-the-hash attacks to move to connected systems, and ultimately gain full domain-level access to—and control over—sensitive data and IT systems.

Spear Phishing Leads to Massive Ukraine Blackout

In December 2015, 225,000 residents throughout western Ukraine lost electricity, and systems belonging to two of the region's utility providers were destroyed. Using a spear phishing campaign against IT admins, the attackers were able to gain the inside access needed to exploit legitimate users, compromise privileged accounts, and ultimately destroy systems and shut off electricity throughout the region.



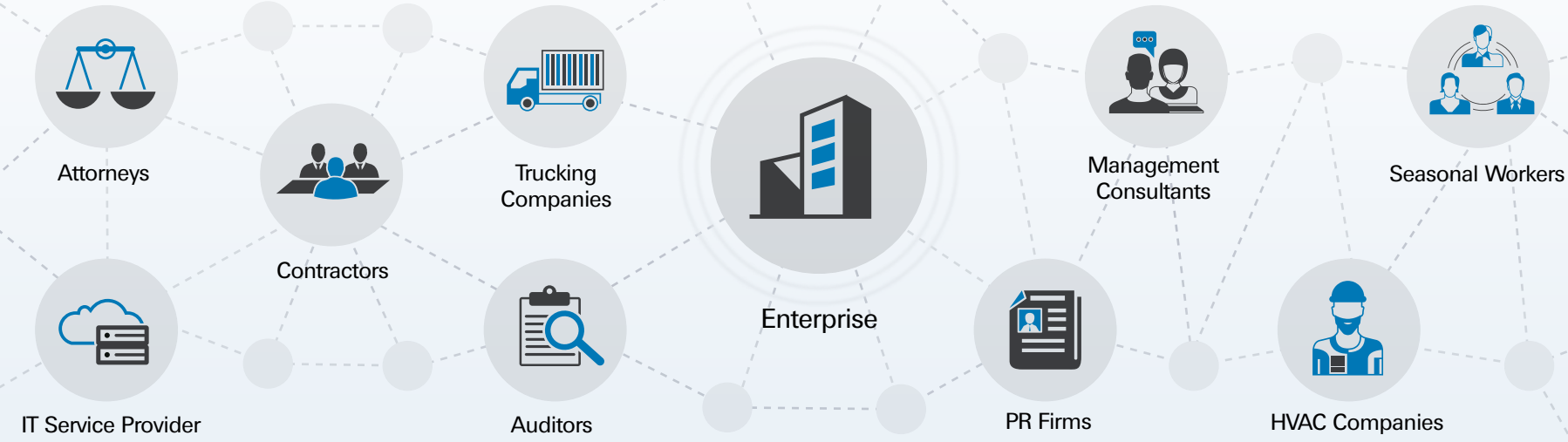
The External "Insider"

At least 60 percent of organizations[3] allow third-party vendors to remotely access their internal networks, and just like employees, these external users can turn into exploited, unintentional and malicious insiders. Yet, these users are not managed by your organization, which makes it difficult to secure and control their privileged access to your resources.

According to a recent survey by the Ponemon Institute, 49 percent of respondents admitted that their organization has already experienced a data breach caused by a third-party vendor, and 73 percent see the problem increasing.[4]

Third-Party Vendor Accidentally Exposes PHI of 665,000 Patients

R-C Healthcare Management has third-party access to hospitals throughout the United States, helping their client hospitals optimize Medicare and Medicaid reimbursements. In April 2016, the vendor attempted to adjust its computer network settings, and in the process, inadvertently made a client's files publicly accessible on the internet. The exposed files contained PHI, PII and bank account information on 665,000 of the client's patients, and the client was forced to publicly disclose the data breach.[5]



The Malicious Insider

Malicious insiders account for just 26 percent of internal incidents,[6] yet they are the most difficult to detect[7] and are the most costly.[8] Malicious insiders—such as disgruntled employees or those in need of financial resources—have knowledge of, and access to, sensitive information and can often legitimately bypass security measures.

Malicious insiders are the most costly.

Malicious Insider Steals Data from 280 Sage Customers

In August 2016, a Sage Group employee was arrested by London Police for suspected fraud. According to Sage, an accounting and payroll software provider, the employee used an internal login to gain unauthorized access to 280 customers and view personal information, salary details, and bank account information on those customers' employees.[9]

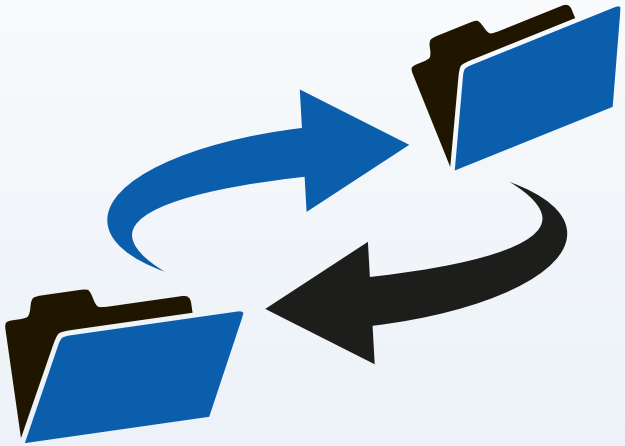
The Unintentional Insider

Most employees are not out to steal sensitive information; they're simply trying to do their jobs. For some, this means storing files in Dropbox or sending information via personal email—actions that may seem harmless, but can unintentionally put data and systems at risk.

In a recent survey from PwC, 50% of organizations reported that their single worst breach during the previous year was attributed to inadvertent human error.[10]

Executive Spoofs Expose PII of Thousands of Employees

In early 2016, attackers sent emails—that appeared to be from the company's CEO or CFO—to finance employees requesting W-2 tax data on all employees. In simply trying to do their jobs, victims at 41 separate U.S. companies complied with the requests and unintentionally exposed personally identifiable information (PII) on thousands of current and former employees.



What Are They After?

Insiders, like all attackers, can have a variety of end goals, but they also all have one thing in common: they target the data and systems to which they have access.

Common End Targets of Insider Attacks:

Information assets (intellectual property, monetizable data)

IT assets (hardware and software that can be corrupted)

Financial assets (money, electronic means to money)

Any asset that sits between the attacker's initial point of access and the attacker's final end goal can be at risk. As such, all data and systems in your organization (especially those that enable lateral movement) are potential targets.

Why Do Insiders Turn Rogue?

Research shows that malicious insiders tend to share a few common motivations:

Anger: They feel as if their employer/manager has done something wrong.

Financial: They have large debts.

Hacktivism: They are motivated by political and religious beliefs.

Outside influence: Their actions are coerced by a crime ring or nation-state.[11]

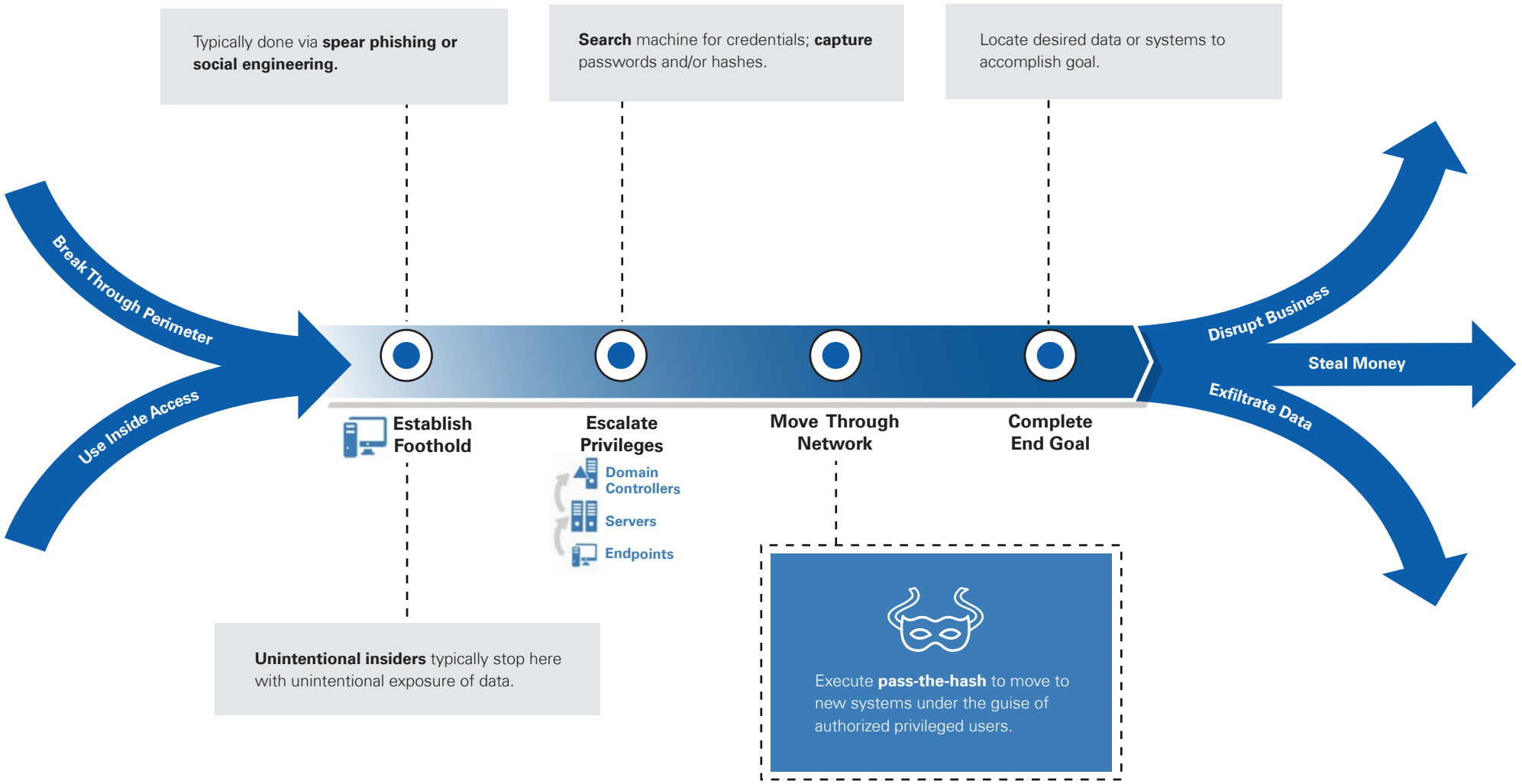
Government Uses Knowledge About Insider Threat Motivations to Detect Risks Earlier

The U.S. Department of Defense created its Insider Threat Programs (ITPs) to track employee behavior and look for life changes that may motivate an employee to steal or damage data. The ITPs track user activity inside and outside of the workplace, aggregating and analyzing data from social media and user devices, to look for indications of drug and alcohol use, financial changes, influence from foreign entities and mental and personality disorders, among other things.[13]

While it's not easy to predict who will go rogue, research points to some key indicators that can help you identify high-risk users prior to an attack. Seventy percent of malicious insiders had been reprimanded for inappropriate behavior—missing work, arguing with coworkers or poor performance—prior to carrying out malicious activity.[12] Organizations can benefit from applying increased scrutiny to such employees.

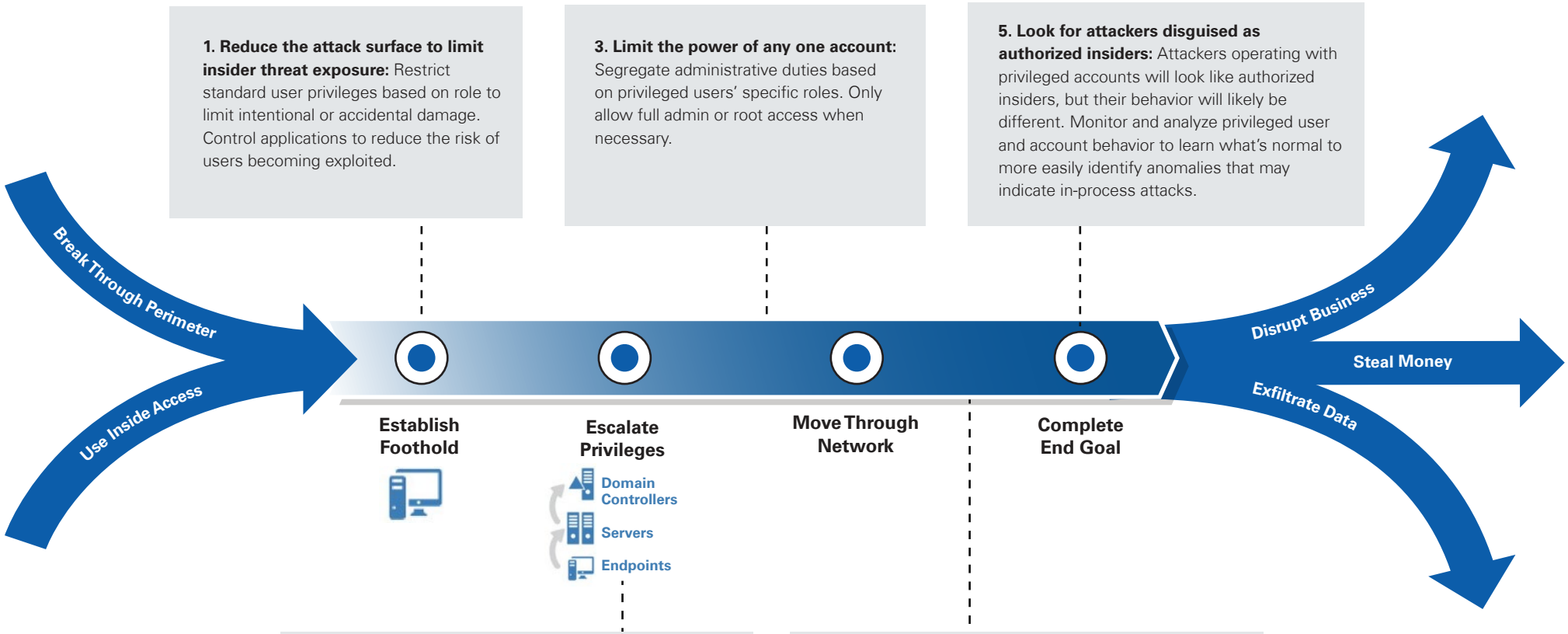
Privileged Access: *How* Insiders Cause Damage

The first step in carrying out an insider attack is to gain inside access. This image shows the typical path attackers follow to complete their mission.



Five Recommendations for Reducing Risk and Quickly Detecting Insider Threats

It's hard to know who may turn rogue, and it's even harder to know who might fall victim to an attack and have their accounts exploited. To reduce the risk of insider threats and limit potential damage, organizations should consider these five recommendations.



1. Reduce the attack surface to limit insider threat exposure: Restrict standard user privileges based on role to limit intentional or accidental damage. Control applications to reduce the risk of users becoming exploited.

2. Don't leave credentials lying around: Store privileged credentials in a secure, central repository that supports strong access controls, multi-factor authentication, and full auditability. Change these credentials on a regular basis.

3. Limit the power of any one account: Segregate administrative duties based on privileged users' specific roles. Only allow full admin or root access when necessary.

4. Do what you can to deter bad behavior: Track the individual use of privileged and shared accounts, and record activity to tie a specific "who" to each action taken. Tell users they are being monitored, and consistently watch for changes in employee behavior.

5. Look for attackers disguised as authorized insiders: Attackers operating with privileged accounts will look like authorized insiders, but their behavior will likely be different. Monitor and analyze privileged user and account behavior to learn what's normal to more easily identify anomalies that may indicate in-process attacks.

Conclusion

When it comes to protecting against insider threats, it's not enough to simply weed out a few "bad apples." To effectively protect against insider threats, organizations should minimize user privileges to reduce the attack surface, lock down privileged credentials, and control and monitor privileged accounts, which are consistently targeted by advanced insider and external attackers alike.

CyberArk's comprehensive solution for privileged account security offers proactive controls to reduce the risk of intentional and unintentional insider threats, as well as real-time monitoring and threat analytics to aid in detection.

To learn more, visit:
www.cyberark.com/solutions/security-risk-management/insider-threats/

CYBERARK®

Sources

[1] "Information Security Forum Examines Security Risks of Insider Threats." Information Security Forum, January 2016.

[2] "The State of Cybersecurity and Digital Trust." Accenture, 2016.

[3] "Global Advanced Threat Landscape Survey." CyberArk, 2014.

[4] "Data Risk in the Third-Party Ecosystem." Ponemon Institute Research Report, April 2016.

[5] "Cybersecurity Attacks Leading 2016 Data Breach Cause." HealthIT Security, December 2016.

[6] "Understand The State Of Data Security And Privacy: 2015 To 2016." Forrester Research, January 2016.

[7] "Verizon 2016 Data Breach Investigations Report." Verizon, April 2016.

[8] "2015 Ponemon Institute Cost of Cyber Crime Study." Ponemon Institute Research Report, October 2015.

[9] "Police Arrest Sage Employee At Airport Following Data Breach" Fortune, August 2016.

[10] "2015 Information Security Breached Survey." HM Government, Conducted by PwC, June 2015.

[11] "Hunting Insider Threats." Forrester Research, June 2016.

[12] "Preventing and Profiling Malicious Insider Attacks." Australian Government Department of Defence, April 2012.

[13] "Defense Contractors Face New Insider Threat Rule." Wall Street Journal, September 2016.

DOC#: 152

CYBERARK®