THE COST OF INACTION

COULD BE DISASTER

Quantifying, Remediating, and Preventing Insider Security Breaches

WARNING

Your organization’s security posture is only as strong as your least secure — or least scrupulous — employee. All it takes is an IT professional forgetting to apply a patch, a manager sending sensitive data to the wrong person, or an angry systems administrator selling your intellectual property to set your business back millions of dollars.

Neglecting to invest in preventative security is one of the most expensive decisions your business can make. And if you think insider attacks or leaks won’t happen to you, think again — the average organization experiences three to four insider security incidents every year, and the average cost of remediation is $450,000 per incident.

That means that employees cost their businesses $1.5 million per year in security cleanup, on average. If that number doesn’t scare you, consider the millions of dollars in fines and possible prison sentences you’ll be exposed to if you run afoul of GLBA, or the penalties and fallout from HIPAA violations.

Let’s take a look at the size of the threat, the legal and financial consequences of insider security attacks, and ways you can prevent potential financial ruin with proactive measures.

THE STATE OF INSIDER THREATS

In 2015, insider breaches accounted for 60% of cyber attacks and drove 80% of total losses to businesses subject to cybersecurity attacks — and as security experts survey damages and trends, the evidence pouring in suggests that the insider threat won't diminish any time soon.

In a more recent survey, 74% percent of organizations feel vulnerable to insider threats. 71% cite accidental breaches as their greatest concern, while negligence (68%) and malicious actors (61%) round out the top three types of insider responses troubling companies the most. Meanwhile, 56% of security professionals report that in the previous year, insider threats at their organizations have become more frequent.

Despite this, only 42% of organizations have the proper controls in place to protect themselves from data leaks and theft coming from their own employees, contractors, and partners — and the same percentage report increased investment in security.

WHO POSES THE GREATEST RISK?

While it may be comforting for CIOs and other IT executives to assume that employees far enough down the org chart — whose intentions and activities may be less well known to the C-suite — account for the majority of insider attacks, the data proves the opposite. Privileged users, such as managers with access to sensitive information, are 60% more likely to cause a data breach, followed by contractors and consultants at 57%. The greater access to data, the greater the possibility of error or malicious attack.

74% of organizations feel vulnerable to insider threats.

71% cite accidental breaches as their greatest concern.

56% of security professionals report that in the previous year, insider threats at their organizations have become more frequent.

60% more likely to cause a data breach are those with access to sensitive information.

42% of organizations have the proper controls in place to protect themselves from data leaks and theft.

II VECTORS OF INSIDER ATTACK

How, exactly, do employees threaten the security posture of the businesses they belong to — and what are the consequences of their actions? While there are many ways to cause a security SNAFU, we can organize insider threats into two basic buckets: malicious activity and unintended error. While the intent of each category of action may differ drastically, the consequences to your business can be equally disastrous.

UNINTENDED ERROR

While it would be naive — and dangerous — to assume that none of your employees would succumb to the temptations of data theft, even the most scrupulous and honorable team member can make an expensive mistake that leaves your data exposed. With accidents like these so easy to happen, it is malpractice not to have adequate controls in place both to prevent unintended breaches and to trace their origins in the event of an error.

Lax security practices lead to data leaks and breaches. Negligence and sheer laziness are unfortunate aspects of the human condition, but in the case of data security, one wrong (or overlooked) move can be catastrophic. Weak passwords, stolen authenticators, cleartext emails sent to unintended recipients, and even forgetting to lock the doors to your server room can cause data to spill out and wreak havoc on your business and reputation.

The infamous Equifax data breach that exposed the social security numbers, credit card data, and borrowing histories of more than 143 million Americans could have been prevented had Equifax security officials patched and updated their systems. While the full impact of this massive leak may take years to add up, the damage to Equifax' reputation is nigh irreparable. Once a pillar of three credit monitoring institutions serving as gatekeepers to borrowers and lenders, this giant has fallen precipitously.

An employee falls victim to malware or phishing. Insiders don't just cause security incidents, but they can open the door to attacks from outsiders whose methods become more sophisticated by the hour. All it takes is an errant mouse click on a sketchy website to download a piece of malware that vacuums up your data. Meanwhile, phishers ply the trade of social engineering — impersonating legitimate organizations via email, phone, or even in-person intrusions — to gather passwords and other means of access to hold your data hostage.

II

MALICIOUS ACTIVITY

This is the most nefarious type of insider threat. Whether for greed, desperation, or anger, an employee may deliberately steal or leak data to achieve a personal end. Here are some of the ways that might occur:

ONE. An employee steals personal or financial data. Your servers and databases house a treasure trove of credit card numbers, bank accounts, social security numbers, and even HIPAA-protected health information, all of which can be weaponized to enrich an employee with access (or the means of obtaining access) or harm members of your organization — or your customers. All it takes is one person with a vendetta, or a desire for extra spending cash, to subject your business to potentially millions of dollars in damages.

TWO. An employee steals your intellectual property. The assets and corporate secrets that keep your organization competitive are the foundation of your financial viability — everything from proprietary research to algorithms worth millions of dollars is up for grabs, and 87% of departing employees take data with them on their way out.

Consider the famous case of Mark Zuckerberg of Facebook and the Winklevoss twins, his partners in a similar project called ConnectU. The twins settled with Zuckerberg for 65 million dollars after he went silent during their partnership, only to "steal" their idea to create what is now Facebook. Like Zuckerberg, any of your employees may privately confess that they "hate working under other people," and make off with your IP.

THREE. An employee damages your reputation by leaking internal documents. Even data leaks whose contents don't result in easily quantifiable financial losses can harm your business, and a disgruntled worker with access to your dirty laundry may seek to damage your public image. And when that happens, fighting the firestorm can be an uphill battle.

When Edward Snowden leaked classified NSA documents, it didn't lead to a sober, nuanced public discussion about the merits of collecting metadata on a mass scale vs. the social costs. Between concerns about privacy and criticism of NSA data security practices that made the leak possible, the intelligence community faced down a burgeoning PR crisis whose reverberations could be felt even in Germany's severing a contract with Verizon.

III

COST OF REMEDIATION

$450,000

is the average remediation cost per incident.

Whether through malice or mistake, the sheer number of ways your employees can compromise your data security is staggering — and with an average remediation cost of $450,000 per incident, even minor vulnerabilities can impact your ability to invest in your business. That six-digit sticker price could go toward recruitment, better technology, or R&D.

But remember that $450,000 is just a per-incident average. Even if you only experience a single breach in the fiscal year, you could be on the hook for a multimillion-dollar cleanup. Before you even get into penalties for non-compliance with regulatory regimes like GLBA or HIPAA, there are three major costs you'll have to worry about after a breach: investigation and forensics, remediation, and public relations.

INVESTIGATION

Forensic analysis of an internal security breach can vary widely in cost, depending on how closely you monitor user activity and how detailed your audit trail is. If you have a well-trained internal response team on-hand, you can find some savings — but if and when it's necessary to call in third-party consultants, you'll begin to see why investing in preventative security pays off. You can expect to pay at least $10,000 just on forensics, but more complex incidents involving savvier insiders or skimpier documentation can easily run up a six-figure bill.

DATA RECOVERY AND REMEDIATION

Once you've determined the source of the breach, you then have to survey the damage, recover what can be recovered, patch your systems, and take measures necessary to make your company whole. Again, the cost of remediation is variable, and much of the final bill depends on your proactive security posture. Do you have secure backup of valuable files? A well thought-out, frequently updated business continuity and disaster recovery plan? These factors help determine how much you'll be paying your security team.

Sometimes, security breaches result in irreparable damage. If an insider sells your IP or corporate secrets, you can't put the toothpaste back in the tube. Once a customer's social security number has been leaked, it's already too late. There's also one asset that can never be recovered: time. As your security team works hard to bring systems back online and restore lost data, your marketing team determines how to get ahead of the crisis, and other key team members divert their attention to fixing the problem, productivity plummets.

CRISIS PR AND NOTIFICATIONS

Depending on your industry, your state's breach notification laws, and your stakeholders, you'll need to invest in crisis communications and make customers aware of the attack.

According to the Ponemon Institute's 2017 Cost of Data Breach Study, United States businesses spent an average $690,000 just notifying customers and stakeholders about major security incidents. Add in reputation fallout, and those costs skyrocket — in the United States, organizations lost an average of $4.3 million in business due to security breaches.

Depending on the size of the injury, you might opt to hire a crisis PR firm to manage your reputation during the remediation process — investing countless thousands just to control the bleeding.

VIOLATION COSTS, FEES, AND FINES

On top of investigation, remediation, and notification costs, you'll also need to worry about the financial penalties of non-compliance with GLBA, PCI DSS, HIPAA/HITECH, and other regulations your industry is subject to. Here's how three common compliance regimes can strike back when your business falls short of their standards.

GLBA

Since 1999, the Gramm-Leach-Bliley Act (GLBA) has required that "financial institutions" (defined as any organization that deals with lending data) follow a specific set of security protocols. Should organizations subject to GLBA expose that financial data, the penalties are more than costly — they can involve prison time. Each individual violation starts at a cool $100,000 fine for the business. Individual employees responsible for the breach have to pay an additional $10,000 per incident and face up to five years of imprisonment for criminal actions.

PCI DSS

The PCI Data Security Standard (DSS) applies to any organization that handles customer credit card information, and requires that companies install strong firewalls, encrypt credit card data, receive regular security assessments, use complex and frequently updated passwords, enforce a strong access structure, and follow other strict security protocols. Falling out of PCI DSS compliance entails a penalty of $5,000 – $500,000, depending on the infraction, while a data breach will set you back $50 – $90 per customer affected.

HIPAA/HITECH

The Health Insurance Portability and Accountability Act (HIPAA) and its more recent sibling, the Health Information Technology for Economic and Clinical Health Act (HITECH), both serve to protect the privacy of an individual's personal health data. While healthcare organizations and insurance companies are familiar with HIPAA and HITECH, these regimes don't just apply to professionals who wear scrubs and stethoscopes — HR departments, benefits managers, and other corporate employees who handle protected health information (PHI) have to abide by certain standards to stay on the right side of the law.

HIPAA/HITECH require organizations to institute physical safeguards (appliance firewalls and locked, monitored server rooms), administrative safeguards, and technical safeguards to stay compliant. Should any of that data leak, the penalties are steep, ranging from $100 to $50,000 per incident, depending on the type of infraction, in addition to possible criminal charges.

IV

INSIDER SECURITY

FIVE BEST PRACTICES FOR PREVENTION

For a deeper dive into each action you should take to assess your threat, read our whitepaper:

Veriato

5 Steps

to Quantifying Insider Risk

5 Steps to Quantifying Insider Risk.

ONE

Quantify your risk. It's important that your security tools, talent, and procedures correspond to your organization's unique level risk. Underinvesting, or choosing the wrong resources, can leave you vulnerable to attack — meanwhile, overinvestment poses its own consequences to your bottom line, so don't install a SCIF in your building until you've determined it's absolutely necessary.

To determine what your business needs to secure against insider threats, you need to involve the right people within the organization, include security onboarding during each new employee's very first day, define the risk each position possesses, align risk levels with everyday controls, and address risk during the termination process to ensure no former employees walk off with sensitive data.

TWO

Establish and enforce strong security policies. Each member of your organization should understand and have a copy of the security protocols and policies they need to abide by. While providing adequate training and knowledge sharing is critical, you should also leave as little to the honor code as possible. Mandate strong passwords and 90-day expiration to force updates, require multi-factor authentication, and lock down file permissions so employees can only access the data they need to fulfill their roles — nothing more.

IV

THREE

Monitor user behavior. Keep automated usage logs to detect anomalies — like employees trying to open folders they don't have access to, or plugging in a portable media device. This doesn't just thwart insider attacks before they're successfully carried out, but it leaves an audit trail for post-incident investigations and reconciliation, sparing you at least a portion of the financial and legal damages that could result from a breach.

FOUR

Budget for insider threats. CIOs know all too well how difficult it can be to get the rest of the C-suite to budget for adequate security protections — even those that specifically protect against outside threats. Insider protections can be an even harder sell, given that many business leaders take great pride in their corporate cultures and implicitly trust their own. Charitable though this attitude may be, that trust can be misplaced — and when an employee compromises your security posture, they damage far more than your faith in your staff.

That's why it's crucial to communicate the insider risk to key stakeholders so that they understand the threat and set aside enough funding to prevent, monitor, and remediate insider security breaches.

FIVE

Invest in an insider security solution. Once you've quantified your level of insider risk and secured buy-in from key stakeholders, you need to research and vet security solutions that fit your organization's unique needs. For many businesses, that means investing in tools and resources dedicated to protecting against insider attacks, whether driven by malice or error.

VERIATO SOLUTIONS FOR INSIDER SECURITY PROTECTION

For more information about the features and functionality Veriato Recon offers, download the Veriato Recon Datasheet.

Veriato

Veriato® Recon

[illegible]

Veriato Recon

[illegible]

Click for a free trial to see it for yourself.

FREE TRIAL

VERIATO RECON

Veriato Recon combines machine learning and advanced statistical analysis to uncover indicators of compromise traditional preventative security measures miss, so you can protect your organization from insider attacks.

Behavioral Baselines

Veriato Recon watches user activity, and using a combination of data science and machine learning, establishes what normal user behavior looks like. Veriato profiles multiple entities, including users, peer groups, and groups created based on observed behavioral characteristics, enabling greater accuracy in anomaly detection.

Behavioral Groups

After a short training period, Veriato Recon identifies groups of users based on observed behavior to enable more accurate baselines, evaluating behaviors including resource and application access and usage.

Anomaly Detection and Alerts

Veriato Recon applies sophisticated algorithms to identify anomalies that would otherwise go undetected. Anomaly alerts are routed to your SIEM or third party data aggregation solution, and you can also choose to receive alerts directly, with a frequency you control.

> *"One of the biggest challenges when managing the insider threat is balancing security without affecting your employees' ability to do their jobs. Veriato's solution quickly detects possible insider risks and attacks, but doesn't impact on business workflows at all. We aim to offer our clients a total security solution to ensure they are covered from every angle, and Veriato will help us do exactly that."*
>
> *Simon Campbell-Young, CEO,*
> *Intact Software Distribution*
> *(Read Full Article)*

VERIATO 360

For organizations facing a high level of risk, Veriato 360 employee monitoring software provides unmatched visibility into the online and communications activity of employees and contractors. This solution is purpose-built to collect full fidelity data on the activity of the people who interact with your IT resources and information. You control what data is collected and when, and what you can access and review, with granularity and flexibility you configure.

For a deeper dive into the features and functionality Veriato 360 offers, download the Veriato 360 Datasheet.

Veriato

Veriato® 360

Why Veriato?

Click for a free trial to see it for yourself.

FREE TRIAL

Screen Capture

Veriato 360's screen capture records everything on a monitored computer's screen. You define how frequently you wish to capture the screen, from the default of every 30 seconds to as often as every second. In addition to regularly defined intervals, triggers can be used to initiate screen capture or to accelerate the interval at which captures occur.

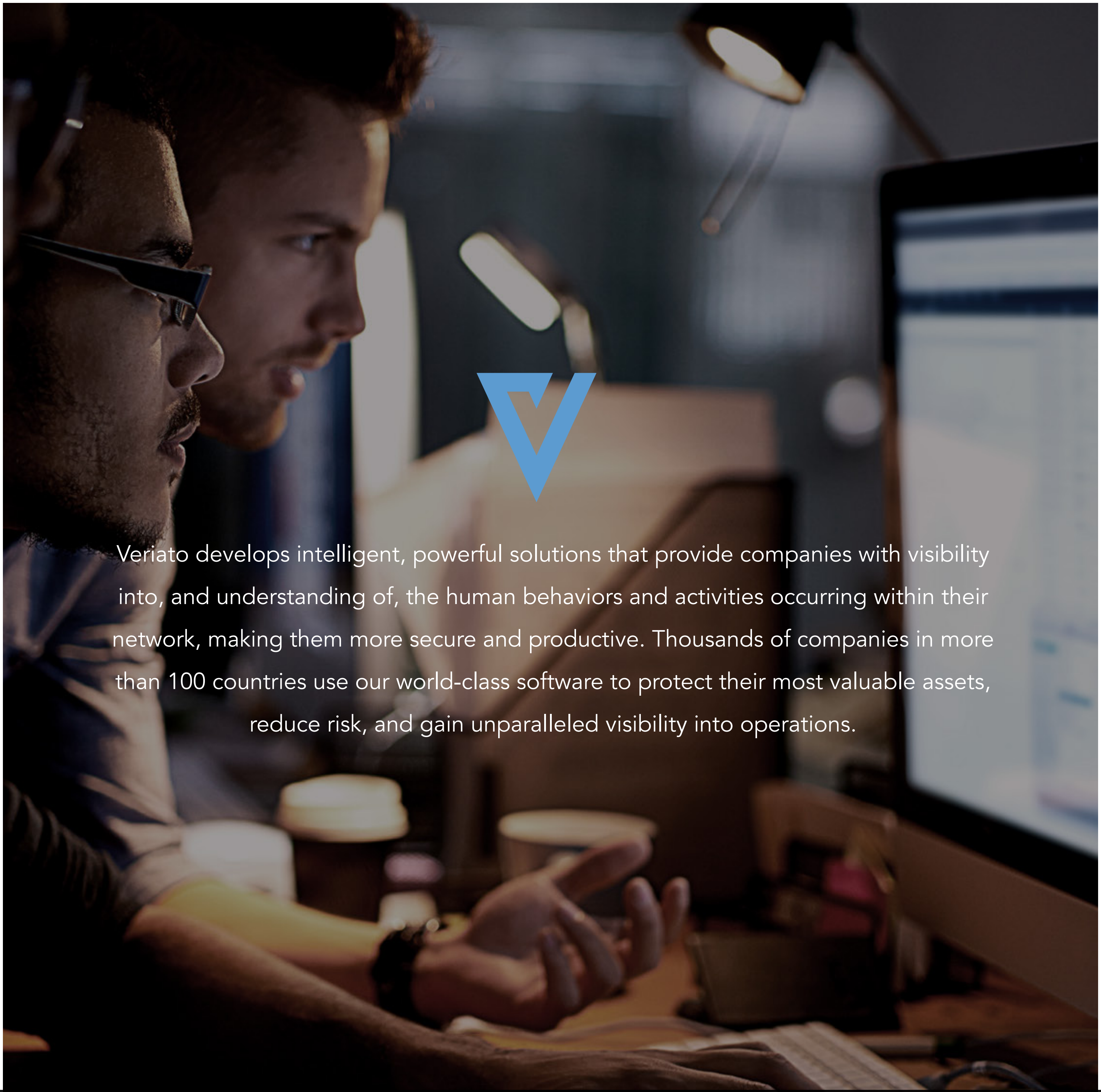
Playback and Review

Video playback of screen activity let's you see exactly what happened, in context. No gray areas — nothing is more effective than pictures. Screen snapshots can be exported as individual BMP or JPG graphic files, and multiple snapshots can be exported together as an AVI video file.

Keystroke Logging

When needed, the option to record every keystroke, including "hidden" characters and combinations, ensures you have the visibility you need into the activity of highly privileged, high-risk users.

> *"I was really amazed at its power and effectiveness. Veriato 360 was the only program with the ability to show us who has opened, edited, and printed a file. With Veriato 360, it was very easy to do, and it gave us so much information."*
>
> *Nick Middleton, IT Manager,*
> *St. Margaret's Somerset Hospice*
> *(Read Full Case Study)*



Veriato develops intelligent, powerful solutions that provide companies with visibility into, and understanding of, the human behaviors and activities occurring within their network, making them more secure and productive. Thousands of companies in more than 100 countries use our world-class software to protect their most valuable assets, reduce risk, and gain unparalleled visibility into operations.

Veriato USA
4440 PGA Boulevard , Suite 500
Palm Beach Gardens, FL 33410

Veriato EMEA
3rd Floor,Crossweys House 28-30
High Street Guildford, Surrey
GU1 3EL United Kingdom