FORCEPOINT
POWERED BY Raytheon

Whitepaper

The Cost of an Unintentional Insider Threat

SUREVIEW® INSIDER THREAT CAN SIGNIFICANTLY HELP MITIGATE COSTS

According to a recent Ponemon report, unintentional employee negligence severely diminishes the productivity of the Information Technology group's (IT) function — IT security practitioners spend an average of almost three hours each day dealing with the security risks caused by employee mistakes or negligence.

Unintentional employee actions, through negligence or simple carelessness, can often lead to a security breach.

INTRODUCTION: INSIDER THREAT WITHOUT THE CLOAK AND DAGGER

When we consider Insider Threat, what usually comes to mind is the malicious employee, motivated by either money or politics, to steal data that can be sold on a black market or used to damage the organization's reputation. We picture scenes of stealthy, underhanded activity including thumb drives, dark offices and a perpetrator plugging in to an unattended computer for the 30-second window that a fellow employee is in the washroom. Whatever the motive, this malicious intent can cause great damage to an organization's finances and/or reputation. But there is another sort of Insider Threat that can cause just as much damage — unintentional actions. Unintentional employee actions, through negligence or simple carelessness, can often lead to a security breach. This is called the Unintentional Insider Threat (UIT). Carnegie Mellon's Computer Emergency Response Team (CERT) offers the following definition of Unintentional Insider Threat:

> *"An unintentional Insider is (1) a current or former employee, contractor, or business partner (2) anyone who has or has had authorized access to an organization's network, system, or data and (3) anyone who, through action or inaction without malicious intent, causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems*[1]*."*

The Unintentional Insider Threat can happen in a myriad of ways. Some include:

- Accidental disclosure or leak via the Internet with sensitive information posted publicly on a website, mishandled, or sent to the wrong party via email, fax, or mail.
- An outsider's electronic entry acquired through social engineering (e.g., phishing email attack, planted or unauthorized USB drive) and carried out via software, such as malware and spyware.
- Improper or accidental disposal of physical records — lost, discarded, or stolen non-electronic records, such as paper documents.
- Lost devices (phones, laptops, etc.) containing confidential information.

According to a recent Ponemon report that compares and contrasts UIT in the United States and Germany, unintentional employee negligence severely diminishes the productivity of the Information Technology group's (IT) function — IT security practitioners spend an average of almost three hours each day dealing with the security risks caused by employee mistakes or negligence. It also causes more security incidents than intentional and malicious acts[2]. A significant number of computer and organizational security professionals believe Insider Threat is the greatest risk to their enterprise, and more than 40 percent report that their greatest security concern is employees accidentally jeopardizing security through data leaks or similar errors[3]. More security incidents are caused by negligence than malicious acts and decrease IT's productivity. (See Figure 1.)

Over the last 12 months, outdated information security controls account for 35 percent of risk exposure, and careless or unaware employees, 38 percent[4]

NEGLIGENCE #1 CAUSE OF INSIDER THREATS

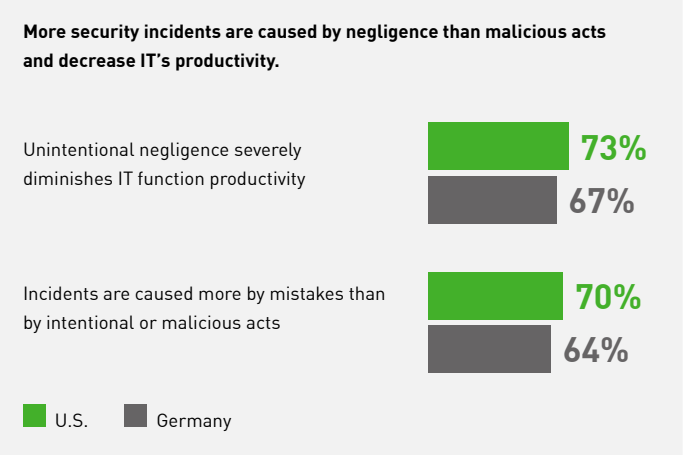

Figure 1 - Negligence #1 Cause of Insider Threats

1 Source: http://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_58748.pdf

2 Source: Ponemon Institute: Unintentional Insider Risk in United States and German Organizations, June 2015

3 Source: Software Engineering Institute: Unintentional Insider Threats: a Foundational Study, August 2013 http://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_58748.pdf

4 Source: 2014 survey by Ernst and Young: Get ahead of cybercrime EY's Global Information Security Survey 2014 http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf

FACTORS THAT CONTRIBUTE TO HIGH UIT LEVELS: TOO MUCH TO DO IN TOO LITTLE TIME

The high rate of Unintentional Insider Threats (UIT) sheds light on the demands of today's workplace culture in the United States. First, employees are being asked to multitask at unprecedented rates. Multitasking has become the norm and, while many workers pride themselves on being good multitaskers, the research shows that actually no one multitasks well and that it comes at the expense of productivity and efficiency. Psychology Today suggests that when we multitask, we lose 40 percent of our productivity[5], are prone to more errors and actually take longer to complete tasks when constantly switching back and forth between them.

Unintentional Insider Threat (UIT) Factors

1. Multitasking
2. Burnout
3. Low situational awareness

Secondly, the American worker has fairly strict limits on vacation time and receives the least amount of paid vacation time in the world[6]. The highly-stressed, multitasking American employee also seems to have lost the traditional lunch break during the day, often eating lunch at his or her desk or on-the-go[7]. Most workers do not take adequate time to rest their brains from the frantic pace of the workplace, which causes burnout and leads to sloppiness in organizational protocol.

Thirdly, although most organizations have mandatory security training programs that teach employees how to prevent accidental data leaks, many still do not. A 2014 Forrester study reported that 42 percent of the North American and European Small to Medium Business (SMB) workforce surveyed had received training on how to remain secure at work, while 57 percent said that they were not even aware of their organization's current security policies[8]. When a training program is in place, its effectiveness is limited when the worker is juggling four or five different tasks at a time, including taking the training module. Security training is often not taken seriously by employees and they go through the motions just to achieve the minimum score needed to pass the test. The information literally goes in one ear and out the other and is never applied, or at least not applied well.

All of these factors lead to low levels of situational awareness. When an employee is preoccupied trying to manage multiple projects, is unable to reinvigorate their brains adequately, and has poor security training, they are less likely to implement the best security practices. These employees are ripe for phishing attacks and are also likely to be careless. For example, an employee might email sensitive information to a personal email address, lose a thumb drive or personal device, or share passwords with co-workers. The main culprit in UIT is the worker who is not situationally aware due to a workplace culture with too much stress and too little training.

THE COST TO THE BUSINESS

Security incidents caused by negligent employees are expensive in terms of time and money. The 2015 Ponemon study asked respondents how much money could be saved if employee negligence was reduced. If negligence was reduced by as much as 50 percent, an average of 31 percent (U.S.) or 28 percent (Germany) of IT security spending could be saved and perhaps allocated for investments in people and enabling technologies. A 25 percent reduction would save 20 percent in the U.S. and 19 percent in Germany in IT security spending. If an organization was able to have a 75 percent reduction, the savings could be as much as 39 percent and 37 percent in U.S. and German organizations, respectively.

Reduced negligence = higher productivity and lower IT spending

5 Source: https://www.psychologytoday.com/blog/brain-wise/201209/the-true-cost-multi-tasking

6 Source: http://www.dailymail.co.uk/news/article-2730947/Americans-paid-vacation-time-world-countries-enjoy-FORTY-days-year.html

7 Source: http://www.today.com/news/americas-lunch-hour-endangered-list-6C9677205

8 Source: Forrester: Understand the State of Data Security 2014 https://www.forrester.com/Understand+The+State+Of+Data+Security+And+Privacy+2013+To+2014/fulltext/-/E-RES82021

REDUCING NEGLIGENCE

How much IT security spending could be saved if employee negligence was reduced by as much as 50 percent?

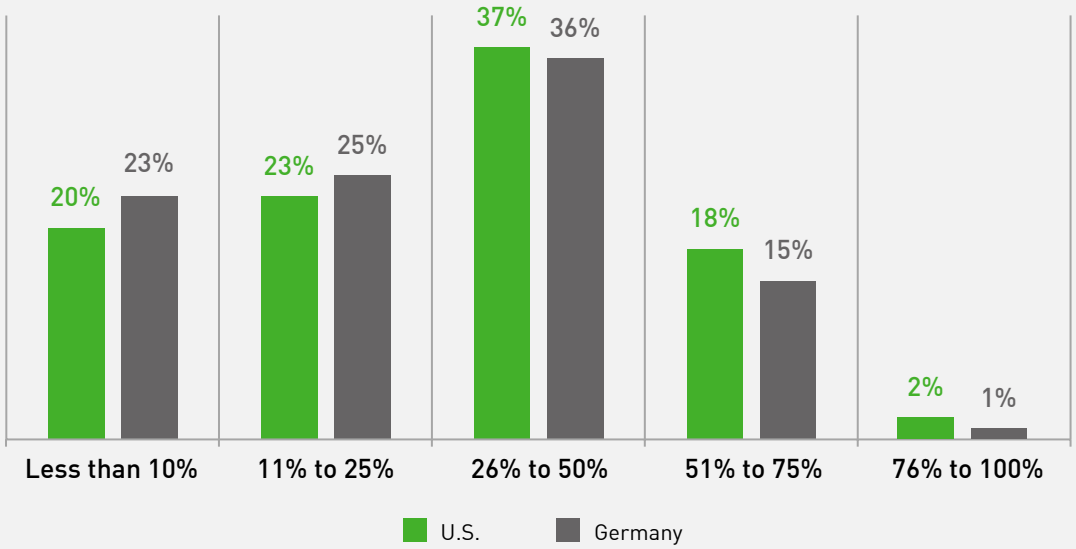

Figure 2 - Reducing Negligence

The burden of monitoring and cleaning up after employee mistakes falls on the IT department and it is estimated that IT workers spend upwards of three hours per day dealing with security risks caused by employee carelessness. Realizing savings in this area will enable IT staff to be more productive, invest resources to increase security expertise and benefit from more investment in technology.

The Ponemon study, which compares UIT in the United States and in Germany, calculated the cost of time wasted responding to security incidents caused by human error in the U.S. to be as much as $1.5 million for a U.S. company and €1.6 million for a German company. For each record compromised due to employee negligence, the average cost is $198 in America and €145 in Germany[9]. These numbers do not include the less-tangible losses from damage to reputation that can affect sales numbers for many months. Even though important to consider, IT cost is a fraction of the overall cost of UIT to the organization.

IT SECURITY COST DUE TO NEGLIGENCE
$1.5 million for a US company and
€1.6 million for a German company

THE AVERAGE COST PER RECORD IS
$198 and €145 in Germany

$400 MILLION:
The estimated financial loss from 700 million compromised records as reported in the 2015 Verizon Data Breach Report[10]

9 Source: 2015 Cost of Data Breach: United States and Germany, sponsored by IBM, May 2015

UNITED STATES AND GERMANY: A CULTURAL STUDY OF UNINTENTIONAL INSIDER THREAT

In the 2015 Ponemon Institute study, U.S. and German employees responded to a set of questions that measure and compare attitudes toward Unintentional Insider Threat. Germany was chosen as they are known, like the U.S., to hold a strong security posture when it comes to IT operations. The purpose of the study was to determine if workplace cultural differences have an impact on the number of UIT breaches and how each country manages this risk.

The study found that 6 percent more respondents in the U.S. felt that unintentional employee negligence severely diminished the productivity of the IT function than in Germany. And 6 percent more U.S. respondents felt that there are more security accidents due to UIT than to intentional and malicious acts (Ponemon considers a 5 percent difference to be significant). Other interesting findings include:

- In Germany, the main culprit of UIT is contractors or other third-party relationships, whereas in the U.S., the main culprit is ordinary users/employees.
- 44 percent of German respondents and 49 percent of U.S. respondents claim they have trouble telling the difference between malicious and non-malicious incidents. For those that can tell the difference, in the U.S. the unintentional incident accounts for 70 percent of all insider security incidents. In Germany, they account for 63 percent.
- German respondents are more likely to agree that their organizations do not have the necessary safeguards in place to protect the organization from careless employees. U.S. respondents are more likely to agree their employees are not properly trained to follow data security policies.

When it comes to workplace culture, the first important aspect to note is that the German work-week is shorter (35 hours expected) than the typical U.S. work-week (40 hours expected). When considered on a daily basis, that is an extra hour of time per day not spent at work and instead spent at rest or with family or other personal pursuits. The German worker also takes a month of vacation per year and is given 6 weeks total in paid vacation[10], where the U.S. worker is typically given half that amount of time or less.

Not only do German workers receive more paid time off, the German culture expects that workers are entirely disconnected from their jobs during that time. In the U.S., the culture is quite different. Many U.S. workers are never really disconnected, and may be reading email and keeping up with company business while on vacation.

Are German workers more productive and efficient in the workplace than U.S. workers because their work culture allows more disconnected time? Does that foster an environment with less

DETERMINING INTENT

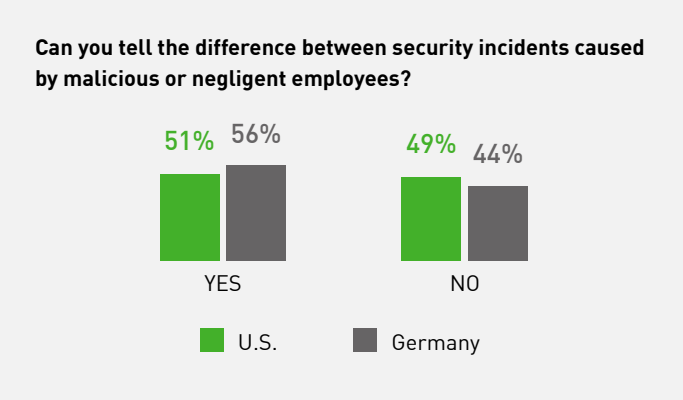

Figure 3 - Determining Intent

expectation to constantly multitask and promote more situational awareness? Probably. But there are also cultural differences in work style that may attribute to a more efficient and less negligence-prone work environment. In the German workplace, the focus is to work at all times during the work day with little or no tolerance for personal or casual conversation or Internet meanderings to Facebook or personal email contact.

This is less so in the U.S., where casual conversation is often weaved into the work day along with time spent on social media or personal communication. If U.S. workers limited these personal interactions throughout the work day, it could increase productivity and therefore more time off [11]. Interestingly, U.S. respondents show a higher level of concern about UIT in their organizations than the German respondents, and coincidentally they also report higher workplace stress levels.

49 percent of all unintentional breaches occur because of accidental disclosure or leak via the Internet.

10 Source: https://www.americanexpress.com/us/small-business/openforum/articles/why-germans-have-longer-vacation-times-and-more-productivity-1/

11 Source: https://www.americanexpress.com/us/small-business/openforum/articles/why-germans-have-longer-vacation-times-and-more-productivity-1/

PROTECTING ASSETS AND EMPLOYEES: UIT SOLUTIONS

It is unlikely that the U.S. or German work cultures will change anytime soon. But regardless of the culture, there are tools and programs that can help any work environment with a UIT problem. Technology can help organizations face IT challenges. Tools like SureView Insider Threat can significantly help mitigate the costs to an organization from the Unintentional Insider Threat.

SureView Insider Threat frees the IT worker to spend valuable time working on projects that support the business versus responding to security incidents that didn't need to happen in the first place.

- **The Stressed-Out Employee.** If long hours and multitasking remain the norm in the U.S. workplace, then SureView Insider Threat will help to mitigate security incidents through monitoring the enterprise with a policy platform that aggregates all relevant data to a dashboard view. There are targeted policy packs based on business policies and best practices for detecting and deterring Insider Threats, such as privileged user abuse, PCI compliance, HIPAA, and more. SureView Insider Threat analysts have the ability to succinctly define policy-based criteria to select which behaviors are audited and what information is collected, unlike other solutions that use a one-size-fits-all approach. This flexibility enables the analyst to easily adjust the criteria for defining a high-risk behavior or a policy violation to meet organizational needs. Every adjustment by the analyst is also audited by the tool to ensure policy compliance and prevent abuse. Equally important, SureView Insider Threat enables analysts to define what sensitive information not to collect, such as user passwords, Social Security numbers, online bank account numbers or confidential and privileged email communication.

- **IT Department Productivity.** In the Ponemon study, 73 percent of U.S. respondents and 63 percent of German respondents stated that unintentional employee negligence severely diminished the productivity of the IT function. With SureView Insider Threat in place, the IT worker is able to spend valuable time working on projects that support the business versus responding to security incidents that did not need to happen in the first place. Simplified policy management and less reliance on a high level of technical expertise helps IT workers accomplish more in less time.

- **Knowing The Difference.** Over 50 percent of the Ponemon respondents reported that it is often difficult to tell the difference between malicious and accidental Insider Threats. SureView Insider Threat's full-context video replay feature enhances the ability to detect negligent vs. malicious activity. The solution provides incident replay including full event end point video recording and custom applications. A different response is needed for a malicious attack versus an innocent and careless mistake. SureView Insider Threat helps ensure the appropriate response which saves calling in the cavalry to fight a mouse.

REDUCING SECURITY INCIDENTS

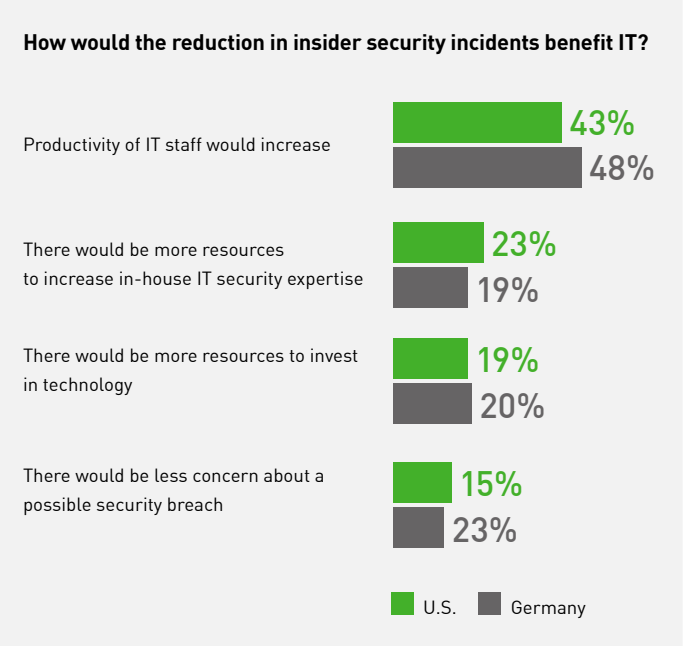

Figure 4 - Reducing Security Incidents

- **Situational Employee Training.** SureView Insider Threat helps to train employees in real time with pop-up windows that display questionable actions and policy violations. For example, if an employee tries to download sensitive data to a USB drive, a window will display alerting them to the potential violation and asking them to verify the action. This helps the unmalicious user understand and learn from their mistakes in real time which is typically more effective than learning through training modules. It also provides support to the employee in the form of a safety net against actions for which they could be reprimanded.

50 percent of the Ponemon respondents reported that it's often difficult to tell the difference between malicious and accidental Insider Threats.

CASE STUDIES

Example One. In this actual SureView Insider Threat customer scenario, we see how SureView Insider Threat helped determine negligence versus malicious acts as well as a malicious perpetrator.

A Fortune 100 Bank was losing a lot of money because of early withdrawal fees associated with Certificate of Deposit (CDs). They were not sure what was happening. Was there a malicious insider stealing? Was it a training issue? The bank implemented SureView Insider Threat and was able to determine that many tellers were being nice and forgiving the fees to customers. The bank put all tellers through CD withdrawal training and the lost-fee incidents dropped dramatically. They also used SureView Insider Threat to provide situational awareness; when a teller attempted to forgive a fee, a pop-up window displayed to remind them of company policy. The training and situational awareness provided by SureView Insider Threat significantly reduced the rate of lost fees. The bank then put a policy in place that required a manager's signature to forgive a fee and the incidents dropped to almost zero. Ultimately there was a malicious actor also detected and removed from the company.

SureView Insider Threat's full context video replay feature enhances the ability to detect negligent vs. malicious activity.

With close to half of all Ponemon survey respondents from both countries reporting that they cannot tell the difference between security incidents caused by employees who are careless and those who are malicious, SureView Insider Threat helps organizations quickly apply the right response to the perceived threat.

Close to half of all Ponemon survey respondents from both countries reported they cannot tell the difference between security incidents caused by employees who are careless and those who are malicious.

Example Two. In this nefarious case, a high-level employee was duped by a phishing scam. They did not have SureView Insider Threat in place and the organization was compromised as a consequence.

Hackers spied on the habits of the CEO of a large organization and waited for an opportunity. When the CEO's son's school was placed under lockdown because police were looking for a criminal at large in the community, the hacker sent a phishing email from "the school" with an attachment containing lock-down procedures. The attachment was a malicious PDF, but it had all the right information, including the letterhead of the private school. The CEO opened it, read the information and never suspected a thing. Hackers gained access to the CEO's computer and the corporate network through this malicious file. It remained undetected for months.

If SureView Insider Threat had been deployed, it would have defended the CEO's email by forwarding suspicious attachments to Threat Protection for Linux before he could have opened it. This was a seasoned executive duped by a clever hacker waiting patiently for just the right scenario to give them an opening. This example shows why it is so important to have protective technologies in place.

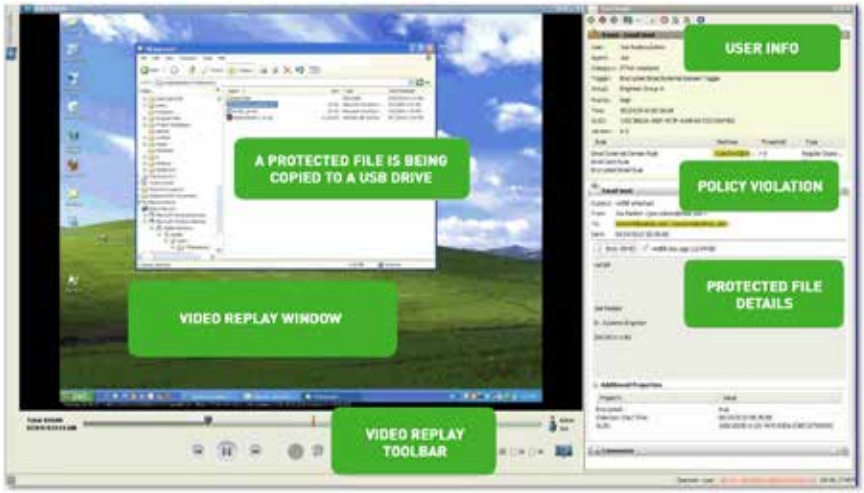

Figure 5 - SureView Insider Threat Investigator Workbench

CONCLUSION: PROTECTING THE ORGANIZATION FROM ITS GREATEST ASSET (EMPLOYEES)

If it was possible to lower stress in the work environment and increase overall situational awareness, many would agree that the number of UIT incidences in the U.S. would reduce. As seen in the comparison with the German workplace environment, today's American worker is working more hours to make up for less efficiency. This is hurting employee situational awareness resulting in increased UIT. And the threat may be growing.

In Verizon's 2015 Data Breach report, Insider Threat occurrences were greater than the year prior, with "end-users" beating out "cashiers" for the first time as the no. 1 offender. According to the report, the end-user accounts for 37.6 percent of negligent incidents, with cashiers trailing in second place at 16.8 percent[12]. In the face of such numbers, it becomes more and more important to establish guardrails around employee activity with a technology solution such as SureView Insider Threat. As well-meaning as employees may be, the average employee, for multiple reasons that include too much multitasking and too little training, lacks a strong and situationally aware security stance. Protection in the form of a monitoring and governance solution will help mitigate UIT and the expensive consequences of compromised internal assets.

12 Source: Verizon 2015 Data Breach Report: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015_en_xg.pdf

CONTACT

www.forcepoint.com/contact