Dtex systems

2018 INSIDER THREAT INTELLIGENCE REPORT

Insights and case studies from Dtex's unique user behavior intelligence and insider threat experts.

THE 2018 INSIDER THREAT INTELLIGENCE REPORT

INSIDER THREATS REMAIN TO BE A GROWING PROBLEM IN 2018 — AND THEY SHOW NO SIGNS OF SLOWING DOWN.

If one theme has snapped into public focus in recent months, it's that people have a messy relationship with technology – and more importantly, that both people and technology are imperfect. With this in mind, it's no great surprise that despite increasing investment in security tools, organizations are still getting breached. In fact, the 2018 Verizon Data Breach Investigations Report recorded over 53,000 total security incidents and 2,216 confirmed breaches. They attribute nearly a third – 28% – of those breaches primarily to internal actors... and that does not even include situations in which internal mistakes or negligence allowed an outside actor to steal data.

THE 2018 VERIZON DATA BREACH INVESTIGATIONS REPORT RECORDED 2,216 CONFIRMED BREACHES, ATTRIBUTING NEARLY A THIRD OF THOSE PRIMARILY TO INSIDER ACTORS.

The good news, however, is that organizations are learning more about how important it is to address the human element. We've seen a massive change in attitudes over the past several years as organizations come to realize that people – not solely machines – are the root of modern cybersecurity. However, this year it has become glaringly obvious employees haven't yet fully realized the extent of that responsibility.

In fact, our recent study with YouGov revealed some contradictory attitudes among employees. While in many cases, employees were able to identify important security behaviors, they frequently didn't follow those behaviors themselves. For example, 75% of respondents identified using an encrypted file system to share confidential documents as important, but only 16% had done so in the past 60 days. The survey found similar results across many other critical security behaviors, like updating anti-virus software (85% identified it as important, but only 37% had done so), using dual-factor authentication (69% vs. 30%), or changing their work login credentials (71% vs. 42%).

But despite the fact that employees knew they weren't doing everything that they could to protect organizational security, nearly a quarter of respondents (23%) still said that they thought their organization's information would never be compromised – proving that many employees don't feel a strong sense of personal responsibility for company security.

Time and time again, we see that while employees understand their inherent vulnerability as a modern user of technology, they still have absolute trust in the organization to protect them and their data. While both of these attitudes come from reasonable places, neither encourage employees to actively engage with organlizational cybersecurity.

EMBRACING THE SHADES OF GREY

Dtex's findings this year fall in line with these attitudes. Our analysts and risk assessments find that negligent or uneducated users are by far the most common risk to sensitive data, confirming that users are not taking responsibility for organizational security – even if they don't realize that they're doing anything wrong.

We group insider threats into three main categories:

Malicious Users - These are users that intentionally harm the enterprise, whether that be in an extreme way (like theft or sabotage) or, more commonly, out of laziness or apathy.

Negligent Users - These are users that harm the organization due to their ignorance, carelessness, or plain human error.

Infiltrators - These are outsiders who infiltrate the organization by taking over insider accounts, often through phishing or credential theft.

However, as this report will soon illustrate, every category of activity we discuss will include many shades of grey – no section is solely attributed to malicious intent or negligent intent or something in between (often the pursuit of convenience, or ignoring security hygiene that users see as "not a big deal"). Out of those shades of grey, a picture will start to emerge that illustrates how users' sense of responsibility for cybersecurity – or a lack of – shapes the threat landscape.

But companies are struggling to answer the question of how to protect against this human factor. Security methods are faltering as organizations increasingly realize that rule-based solutions can't protect against all internal threats, and can't see the threats that inevitably slip through the cracks. IT teams grapple with hundreds of unactionable alerts per day, but still aren't getting the answers that they need to stop these threats. And that's only if the tools in question are scalable enough to deploy enterprise-wide to begin with – which oftentimes, they aren't.

What's more, the critical balance between security and privacy is increasingly being called into the public consciousness. In the EU, the General Data Protection Regulation (GDPR) has forced companies to completely re-evaluate how they collect, store, and use employee information. Last summer, a judge in Germany ruled that using a keylogging software to monitor employees is against the law. But even in countries like the US, which currently has very few privacy laws, the tide is turning. The ongoing scandal about Facebook's data collection has more and more average people thinking about their privacy – and voicing their displeasure with the idea of invasive monitoring of any kind.

The biggest challenge that organizations will face in 2018/2019 is learning how to build security infrastructure around the unpredictable human element – especially as users become more intolerant of surveillance, rule-based tools fail to account for the unknown-unknowns, and noisy data sources struggle to pinpoint actionable insights. This year's data proves that the sheer variety of ways that human threats put the organization at risk – whether intentionally or unintentionally – require organizations to rethink their security approaches and answer the questions that really matter.

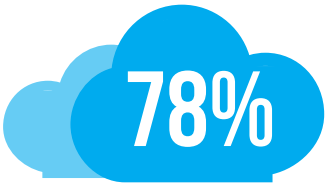
THE BIGGEST CHALLENGE THAT ORGANIZATIONS WILL FACE IN 2018/2019 IS LEARNING HOW TO BUILD SECURITY INFRASTRUCTURE AROUND THE EVASIVE HUMAN ELEMENT...

...ESPECIALLY AS USERS BECOME MORE INTOLERANT OF SURVEILLANCE, RULE-BASED TOOLS FAIL TO ACCOUNT FOR THE UNKNOWN-UNKNOWNS, AND NOISY DATA SOURCES STRUGGLE TO PINPOINT ACTIONABLE INSIGHTS.

HIGHLIGHTS IN FINDINGS

2017's Key Trends, Challenges, and Patterns

Dtex analyzed 2017 risk assessments comparing data and trends to those of previous years. The goal was to highlight key trends in both malicious and negligent behaviors by employees, contractors, and partners that use corporate systems. Top takeaways from this year's report include:

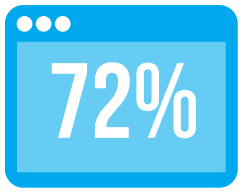


PUBLICLY ACCESSIBLE DATA

78% of assessments found company data publicly accessible online, in a **14% increase** from last year.

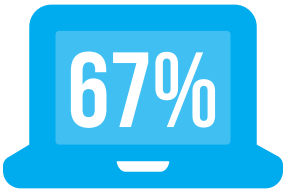
SECURITY BYPASS VIA PRIVATE OR ANONYMOUS BROWSING

60% of assessments found users actively attempting to bypass security measures through private or anonymous browsers and research.



HIGH RISK APPLICATIONS

72% of assessments found unauthorized use of high-risk applications, including hacking tools.



INAPPROPRIATE INTERNET USE

67% of assessments found employees engaging in inappropriate internet usage, such as gambling, porn, etc – an **8% increase** from last year.

HIGH-RISK DATA TRANSFER VIA USB

90% of assessments found company data being transferred to unencrypted USB devices, in a **5% decrease** from last year.

PART ONE

MALICIOUS USERS

Malicious insiders are perceived by many as the “traditional” insider threat: employees who intentionally harm the organization. These are insiders that generally are well aware that they’re doing something wrong, with motivations that can range anywhere from laziness to greed to spite.

1. SECURITY BYPASS
2. HIGH RISK APPLICATIONS
3. LEAVERS AND JOINERS
4. CREDENTIAL MISUSE
5. PIRATED MEDIA
6. INAPPROPRIATE INTERNET USE

SECURITY BYPASS

A key indicator of user intent.

The tricky thing about dealing with human-based threats is determining intent. Even if an organization can detect a singular security event, that one piece of activity doesn't mean much until it is painted in the full color of the context that surrounds it. Negligent or unintentional threats require a much different response than malicious acts, so in these situations, background is critical. Our analysts find that the number one way to determine whether an act was malicious is to see whether it is preceded by a blaring red flag: attempts to bypass company security.

When an employee takes the time to actively bypass security measures, it's because they know that they're doing something wrong. While sometimes they do this for sinister reasons like data theft, we most commonly see employees circumvent security measures in order to cut corners. However, even in relatively petty cases, these users often fail to understand how bypass puts the organization's security – and their own security – at risk.

of assessments saw users utilizing anonymous or private browsing in order to bypass security, or researching how to bypass security measures.

SPOTLIGHT TRENDS: IN-PRIVATE MODE AND OFF-NETWORK ACTIVITY

Dtex's analysts noticed a growing trend this year of employees adopting In-Private browsing mode (such as Chrome's Incognito mode) before committing other unsanctioned activity. Many employees think that In-Private browsing mode shields their activity, but, at least in Dtex's case, that is not true. We saw use of In-Private mode for activity like researching circumvention tools, personal email, downloading hacking tools, and generally inappropriate internet activity. While In-Private mode alone is not dangerous and doesn't *actually* hide user activity, it's worth it to have visibility into this activity if only because so many people *think* it does. As a result, it can be an early indicator for subsequent risky activity... and, potentially, malicious intent.

Similarly, we also regularly see users taking their devices off of the corporate network to engage in risky activity. Oftentimes, users believe that their employers have limited visibility into off-network activity – an assumption that, depending on the company's security posture, might be true. Malicious activity often takes place while the user is at home or on public wifi. This is why it is so important that organizations have visibility into off-network behavior, especially in today's age of distributed enterprises.

THE IMPORTANCE OF DEFENSE-IN-DEPTH

Throughout this report, findings will illustrate the importance of a defense-in-depth strategy based on quality visibility. It is unavoidable that employees will at some point be able to bypass security measures like DLP – whether it be out of outward maliciousness or misconfigured rules. These acts often go undetected without insights into user behavior.

HIGH-RISK APPLICATIONS

Users execute hacking tools, torrenting, and beyond.

This year, Dtex frequently caught users introducing high-risk applications into the organization. This includes applications such as hacking tools, network tools, and other generally risky programs – many of which aren't sanctioned by the organization, or are allowed only for specific members of the security team. Common examples include OpenVPN, uTorrent, WireShark, and similar tools. Like Security Bypass, the use of High Risk Applications is often a warning sign of something worse. A user will typically install such applications so that they can get around security measures, download pirated media, or engage in more sinister activity.

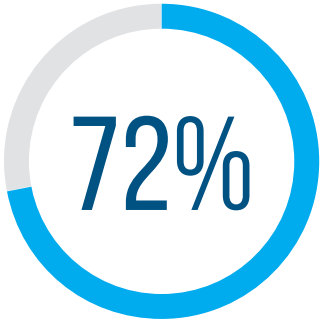
MALICIOUS APPLICATIONS AND SECURITY BYPASS

In many of these instances, users were downloading risky applications to perform administrative functions. Most frequently, users would utilize these tools to circumvent security measures. However, this wasn't aways the case. In some situations, users were unwittingly using unsanctioned applications to accomplish their job.

To combat this uncertainty, analysts used contextual evidence to determine when employees knew that their behavior was disallowed. Downloads taking place in In-Private mode, for example, could be an early indicator of potential security bypass. Another more troubling indicator is the use of portable applications. These were run from USB drives and required no installation, leading users to believe that they were covering their tracks.

A SOLUTION: CLOSE GAPS AND RECOGNIZE WEAKNESSES

Organizations need to place clear guidelines around unsanctioned tools and be sure they can recognize when such rules aren't being followed. Rule-based tools cannot be the only line of defense, since the number of high-risk applications increases exponentially every day – and inevitably, some will slip through the cracks. Dtex customers often had no idea what types of applications were being used in their organization before deployment. This emphasizes the importance of profiling user-based application behaviors to understand normal behavior and highlight outliers, rather than simply relying on white-lists or blacklists.



of assessments saw unauthorized use of high risk applications.

COMMON RISKY APPLICATIONS SEEN IN ASSESSMENTS INCLUDE:

- openVPN tools
- Research on "how to get around security controls"
- uTorrent
- WireShark
- Powershell
- Ccleaner
- snippingTool.exe
- FreeWatch.exe
- DontSleep.exe
- PDF converters – non-adobe, not endorsed
- Caffeine.exe

LEAVERS AND JOINERS

A time-tested narrative is shifting.

One particular version of the leaver/joiner narrative is pervasive: the tale of a disgruntled employee stealing valuable IP from their company after quitting or being fired. For years, this was the only kind of employee risk that companies worried about, and it became the definitive model of what people thought of when they thought "insider threat."

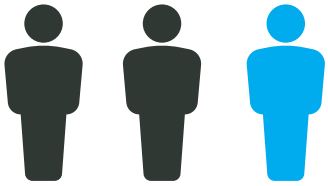
Today, many organizations are rightfully still concerned about this scenario. Roughly one third of assessments (38%) alerted on employees displaying flight risk behavior, indicating higher risk for potential data theft. Once these employees were flagged as high risk, their risk scores were multiplied so that security teams would be more quickly alerted any potentially suspicious behaviors – especially those indicating potential data theft.

However, leaving employees aren't the only high risk users that companies need to be concerned about. More and more organizations are realizing that they need to be conscious of new employees, too – since having stolen data brought *into* their company can be nearly as damaging as data theft, as proven by Waymo's recent lawsuit against Uber. When new employees bring stolen data into the enterprise, companies are open to tremendous legal consequences. The fact that this very scenario cost Uber $245 million has made executives around the world sit up and take notice.

THE RECOMMENDED APPROACH

When it comes to detecting data theft by new or departing employees, having the right technology is critical. Most security tools don't have the visibility to catch stolen data being brought in or out of the organization by these high risk users.

Many of Dtex's customers adopt a period of heightened security for users that are deemed "high risk" – often new employees, flight risk employees, employees that will soon be fired or laid off, or employees that consistently exhibit high risk scores. This status heightens their risk scores to be sure that new employees aren't bringing in legally questionable data, and will immediately flag any sign of potential data theft by flight risk employees.



1 IN 3

assessments revealed employees displaying flight risk behavior, indicating higher risk for potential data theft.

REAL WORLD SPOTLIGHT

JOINERS' STOLEN DATA

Dtex alerts on cases of a new employee bringing large amounts of stolen data into the organization. In the highly-competitive engineering industry, in which developing the most cutting-edge technology can make or break the success of the company, a Dtex customer twice saw new employees importing a large number of design files... which turned out to come from competitors. Luckily, in both of these cases, Dtex caught the import of the stolen data and the company was able to mitigate the situation before it became a legal problem.

CREDENTIAL MISUSE

Casual abuses of power under a shield of privilege.

Credential misuse encompasses any way that a user utilizes their credentials or administrative privileges in a manner that can harm the organization. Last year, we bundled this topic with credential theft. This year, however, it emerged as a distinctly different – and very insider-focused – category.

Dtex's assessments found employees misuse their credentials in a variety of ways. Most commonly, Dtex saw admin users engaging in questionable activity like escalating or granting administrative privileges to their other accounts, or granting those privileges to coworkers. Concerningly, organizations often didn't even know who was supposed to have these privileges and who wasn't.

SPOTLIGHT TREND: HIDING BEHIND A SHIELD OF PRIVILEGE

While many instances of credential misuse were not necessarily malicious, Dtex assessments did observe a trend this year of users using admin privileges as cover for petty wrongdoing. For example, assessments caught users using admin accounts to do things like checking personal email, using torrenting programs, downloading pirated media, and other disallowed activity.

These users seemed to think that using their admin accounts would keep their actions from being monitored – and though that would be true with many security tools, Dtex still alerted on their actions and even ensured that the act of covering tracks through a privileged account made the high risk activity even more obvious. Most of the time, this behavior generally applied to petty wrongdoing, rather than more serious infractions like using privileged accounts to steal company data.

However, that is far from the worst-case scenario. Such escalated privileges can be used to steal data, disable security measures, sabotage or damage IT infrastructure, or commit any other number of crippling attacks – and those outcomes could be even worse if an outside infiltrator were to gain control of these unchecked privileges.

These organizations had no insight into these behaviors, and prior to deploying Dtex, had no visibility into how privileges were being used or shared (as these are not insights that security teams can get from log files or similar data sources). Visibility into privileged user behavior – and which users have these privileges – needs to be a critical priority.

THE MOST COMMON WAYS THAT ANALYSTS SAW ADMINS ABUSING CREDENTIALS:

- **Escalating or granting privileges to their "normal" account or other employees.**
  Organizations often had lax or unenforceable policies around privileged accounts, and had no visibility into which users had privileges and which didn't... or a full understanding of how they were being used.
- **Using admin accounts to cover for petty wrongdoing**
  Some users would switch to their admin credentials every time they violated company policies. This was noted as a recurring problem this year.

WHICH COULD LEAD TO DAMAGES SUCH AS:

- **Disabling security measures**
- **Data theft**
- **Infrastructure sabotage**
- **Unchecked damage if an outside infiltrator gains access to privileged accounts**

PIRATED MEDIA

Casual pirates open organizations to steep penalties.

This year, Dtex assessments caught slightly fewer pirated media incidents than last year – but not by much. Dtex found pirated media on cloud storage, removable storage, and local storage. Multiple Dtex customers found that users were going through great lengths to transfer and obfuscate pirated media between employees. For example, in several organizations, Dtex discovered many users sharing pirated media with each other by transferring from USB drive to USB drive through company computers.

of assessments found pirated software or media in the company network.

This is a

10% DECREASE

from last year's report.

THE POTENTIAL CONSEQUENCES

The presence of pirated media in the company network is a problem for a variety of reasons. It opens the company up to a significant amount of legal risk – the use of pirated software can be punishable by fines of up to $250,000. Pirated media is also often linked to malware. Recent research from Carnegie Mellon found that the more time subjects spent on pirate sites, the more likely they were to have malware on their machines – specifically, each time a user doubled the amount of time spent on pirate sites, the malware count on their machine jumped 20%. What's more, the means that a user has to go through to obtain pirated media typically involves them circumventing security or visiting unsavory websites, which means they're expanding the organization's technological attack surface.

Many Dtex customers didn't even know that their users were downloading, transferring, or using pirated media, meaning that they weren't prepared to mitigate or address that threat

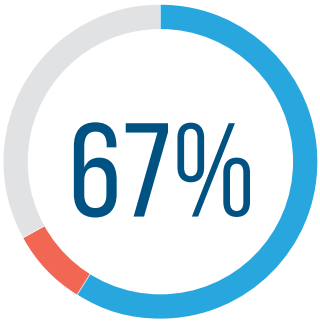
REAL-WORLD SPOTLIGHT: SHARING PIRATE'S LOOT

At one organization, Dtex caught employees using company servers to share pirated media with each other. Users transferred pirated files from personal USBs to corporate network share locations. From there, another user within the company would copy those files to a local desktop folder with an innocuous name, like "Computer System Files" – a clear attempt at obfuscation. That user would then cover their tracks further by deleting the file on the network share after transferring. This process managed to evade detection until Dtex was deployed, opening the company in question up to significant legal risk as a growing amount of pirated media was spread across their organization.

INAPPROPRIATE INTERNET USE

An indicator and a risk, despite a shift in priorities.

Inappropriate internet usage encompasses all internet activity that is generally unsuitable for the work environment, including activity like viewing porn, gambling, playing video games, etc. This year, Dtex saw more and more organizations choose to prioritize areas of security concerns. Security professionals are realizing that protecting everything is protecting nothing, and that placing equal effort into stopping literally every form of security infraction is an impossible battle. As a result, these teams are prioritizing their concerns – and most of them don't place a lot of value on stopping inappropriate internet usage, so long as it's not directly threatening the security of the organization. However, inappropriate internet usage remains to be a loose indicator of other bad behavior, especially if an employee circumvents security measures to do so. What's more, many of these inappropriate behaviors lead employees to websites that are likely to expose company machines to other risks.



of assessments found employees engaging in inappropriate internet usage, such as gaming, gambling, porn, etc...

...in an

8% INCREASE

from last year's findings.

SUCCUMBING TO CRYPTO-MADNESS

This year, analysts noticed an interesting and significant increase in BitCoin activity – likely due to the recent explosion of cryptocurrency interest. Employees are using their work devices to mine, trade, or purchase BitCoin, often during work hours. This activity harmed productivity, and brought users to shady websites that open company networks to malware threats.

REAL-WORLD SPOTLIGHT: AN EMPLOYEE'S REVENGE

Dtex did catch one highly unusual case that didn't quite align with typical inappropriate internet use. A client informed Dtex that a senior staff member had received a barrage of unwanted calls and text messages from injury lawyers and PPI recovery companies. They were wondering whether it was possible to find out, using Dtex, if someone on the senior employee's team had been submitting their information for these kinds of calls, since one of the nuisance emails had mentioned information that would only be known internally.

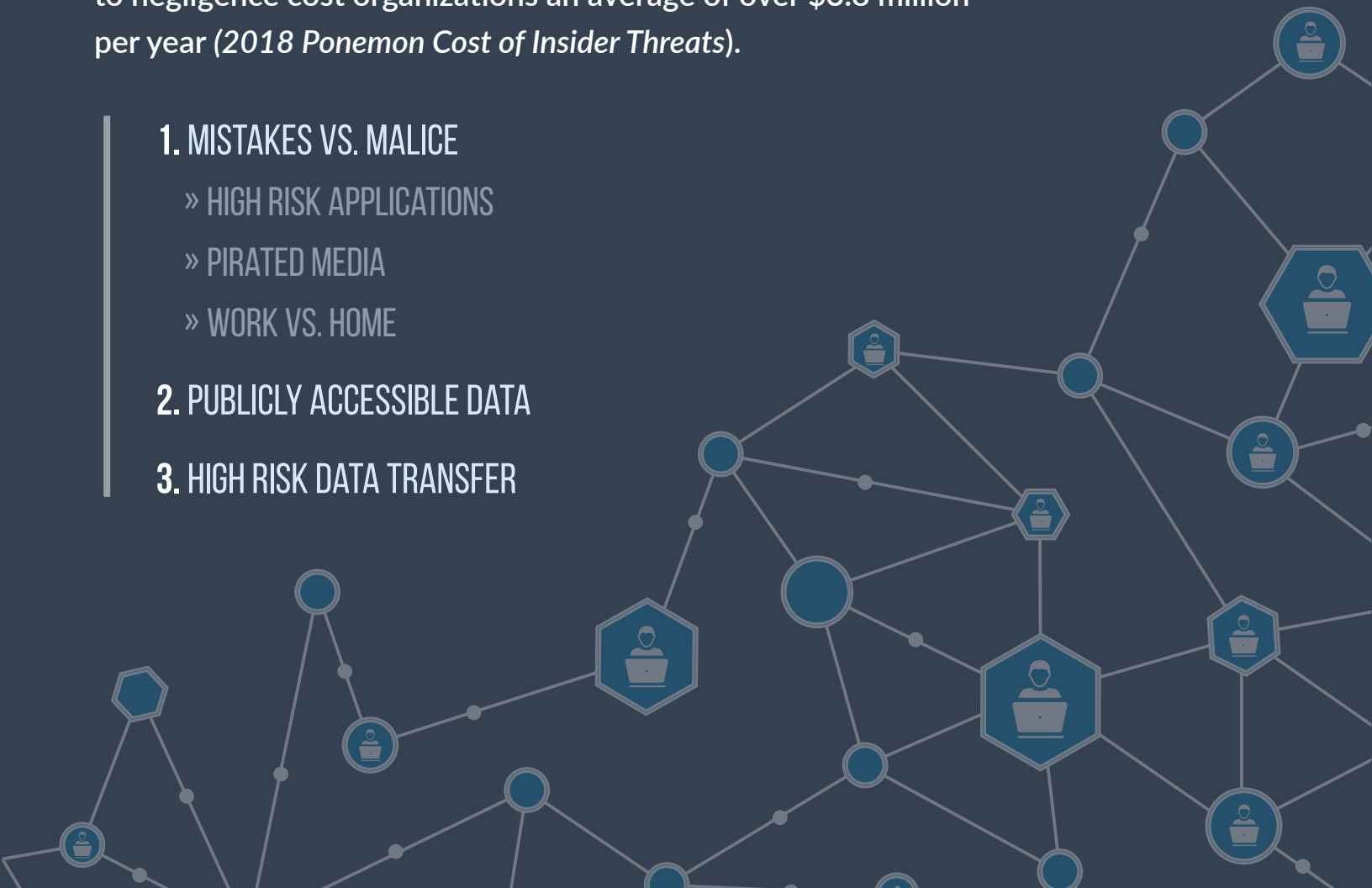
Dtex's investigation revealed that, indeed, one internal employee had been filling out various nuisance forms with their boss's information – and had been performing Google searches for terms like "PPI call back" and "whiplash claim." The employee in question was confronted, and the manager was able to put to rest a mysterious – and annoying – string of events.

PART TWO

NEGLIGENT USERS

As a general rule, negligent incidents are far more common than malicious ones. Negligent insiders are employees that unintentionally put organizational security at risk, often through well-intentioned ignorance, laziness, or simple human error. While many organizations make the mistake of focusing exclusively on would-be malicious data-thieves, insider threat incidents attributed to negligence cost organizations an average of over $3.8 million per year *(2018 Ponemon Cost of Insider Threats)*.

1. MISTAKES VS. MALICE
   - » HIGH RISK APPLICATIONS
   - » PIRATED MEDIA
   - » WORK VS. HOME
2. PUBLICLY ACCESSIBLE DATA
3. HIGH RISK DATA TRANSFER



MISTAKES VS. MALICE

In investigations, context matters.

Before addressing specific categories of actions that lend themselves exclusively to negligent users, it's important to make one thing clear: negligence is by far much more common than malicious intent. In fact, the Ponemon Institutes's 2018 Cost of Insider Threats report found that 64% of insider threat events were attributed to negligent users.

This is why contextual behavioral information is so important. Oftentimes, behaviors that seem like they would be malicious at first glance turn out to be matters of ignorance, laziness, or negligence. Dtex saw this firsthand many times over the course of the year. For example:

> **"NO OTHER DATA BREACH SOURCE CAME CLOSE TO ACCIDENTAL LOSS, WHICH WAS RESPONSIBLE FOR ALMOST 2 BILLION COMPROMISED RECORDS IN 2017 - AN INCREASE OF 580 PERCENT YEAR OVER YEAR."**
>
> *- The 2017 Breach Level Index*

WELL-INTENTIONED MISTAKES: HIGH-RISK APPLICATIONS

In several situations, Dtex caught users introducing risky applications into organizations purely out of ignorance. For example, one assessment found an employee using a virus-laden unsanctioned PDF converter program – one that was found for free on the internet, not produced by Adobe and downloaded from a very suspicious website. The user in question had no intention of hurting the organization. They simply needed a tool and went looking for it on the internet, without knowing how to determine legitimacy. This application was likely malware, but since Dtex found this activity, the IT team was able to mitigate the situation before there was damage.

ACCIDENTS HAPPEN: PIRATED MEDIA

As briefly mentioned earlier in this report, Dtex assessments caught several instances this year where employees were storing pirated media on their personal cloud storage accounts, and unwittingly transferring that media to their work computers via automatic syncing. In many cases, neither the employee nor the organization realized that they were storing illegal media on their work devices until Dtex caught the infraction.

DTEX CAUGHT MANY INSTANCES THIS YEAR WHERE AUTOMATIC SYNCING TO CLOUD STORAGE PUT COMPANY DATA AT RISK OR BROUGHT RISKY DATA INTO THE ORGANIZATION.

TWO WORLDS COLLIDING: AN EXPANDED ATTACK SURFACE

This report already discussed the potential security dangers of inappropriate internet usage on work machines. This year, analysts noted a trend where oftentimes, all flagged inappropriate activity took place outside of normal working hours, and while the device was off of the corporate network. Many employees were using their company devices as their personal devices while outside of the office.

Risk scores for these users were overall much higher, simply because the attack surface is broader – users who use their work devices for all personal activity vastly increase the number of ways that device can be compromised, especially since these out-of-work functions are not protected by organizational security measures.

APPROACHING THE THREAT OF NEGLIGENCE

There are many more examples of these types of scenarios. None of the employees in any of these instances were trying to wage some kind of attack against their organizations. In the vast majority of cases, they didn't even realize that they were doing anything wrong – and if they did, they were doing it out of apathy or a desire for convenience. But that doesn't make their actions any less dangerous. Never underestimate the potential damage that can be done by a negligent user, and always remember that negligence can come in the form of almost every type of bad action, from high-risk application usage to suspicious data transfers, and many more. What's more, a negligent user may not follow the typical insider threat kill chain, which sometimes makes it even more difficult to find threats introduced by those users.

> **IF EVERY USER IS VULNERABLE, HOW DO SECURITY TEAMS FIGHT THAT THREAT? SOLUTIONS THAT REQUIRE SECURITY TEAMS TO KNOW IN ADVANCE WHO AND WHAT THEY'RE FIGHTING AGAINST CANNOT STOP THESE KINDS OF RISKS.**

But this poses an important challenge to organizations today: if every user is vulnerable and can jeopardize security in unpredictable ways, how do security teams fight that threat? Solutions that require security teams to know in advance who and what they're defending against – like rule-based DLP – simply are not capable of stopping these kinds of risks.

This is why it's so important that organizations have the ability to see a clear audit trail of user activity, both on and off the network. Most new Dtex customers are shocked to see the types of things that their employees are doing to jeopardize organizational security, even if they aren't ill-intentioned – and despite heavy investment in security, most of these activities go undetected until Dtex's deployment.

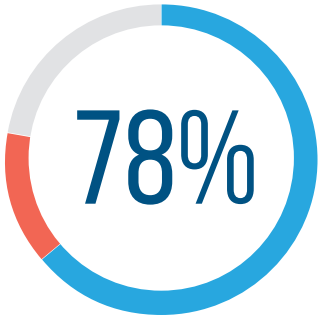
PUBLICLY ACCESSIBLE DATA

Organizations are leaving data exposed – and it will only get worse.

While it hasn't gotten much widespread attention, publicly accessible information was by far one of the most dangerous and widespread issues of the year – and it's a threat that will only grow more common as cloud storage and automatic syncing become increasingly widespread.

In 78% of all assessments, Dtex found company information completely publicly accessible in the cloud – usually on websites like Google Drive (or Docs, Sheets, etc), DropBox, Box, etc. This means that company information – and oftentimes, very sensitive data, like SSNs or financial information – was completely accessible to anyone who had or could find a certain link, no credentials necessary. This is an increase of 14% from last year's report, and the largest increase witnessed in any category of insider activity.

Analysts recognize this as an extremely common and growing problem. The sensitive data that Dtex has found publicly accessible on the internet includes employee data, client data, highly sensitive legal information, and much more.



of assessments found company data publicly accessible in the cloud.

This is a

14% INCREASE

from last year.

WHY DOES IT MATTER?

Anyone at all with a certain URL can access these sensitive documents. Analysts even frequently observed messages like, "Last edited by Anonymous" on sensitive company documents, which means that the organization couldn't tell who had last edited the doc – or if it was even an employee. There was no way to know who had viewed or changed it.

What's more, this introduces another danger that's slightly less obvious: phishing. Companies who do not have clear policies around file sharing sites tend to have more phishing incidents because many phishing emails mimic alerts from popular cloud sites – such as DropBox, Google Drive, or Box. Since employees at these companies use any and all file sharing sites, it wouldn't seem strange or suspicious to them to get notifications from any of these websites – meaning that they are far more likely to fall for one of these phishing emails.

> **"IN TWO YEARS AN AVERAGE OF 51 PERCENT OF ALL IT AND DATA PROCESSING REQUIREMENTS WILL BE IN THE CLOUD, AN INCREASE FROM TODAY'S AVERAGE OF 39 PERCENT. ON AVERAGE, COMPANIES ARE USING 27 CLOUD APPLICATIONS."**
>
> *-The 2018 Global Cloud Data Security Survey, Ponemon Institute*

A GROWING RISK WITH NO SIGNS OF STOPPING

Why is this such a growing issue? There are a few reasons:

1. **Cloud storage is becoming more common -** In 2013, Apple iCloud became the most-used cloud service in the US, with 250 million active users. In 2016, iCloud had 782 million users, more than tripling its figure in just three years – and that's just *one* cloud service. Now, almost everyone uses some form of cloud storage, even people who aren't particularly well-versed with technology. In many cases, these are the people who pose the most risk, since they aren't always sure what sharing cloud media means or how to keep track of privacy settings.

2. **Employee's phones or personal devices automatically sync -** This is a growing problem as it becomes increasingly common for devices to automatically sync to the cloud. In many cases, users don't realize that their cloud accounts automatically sync to desktops, or understand fully how to manage these settings. Even for those who are more tech-savvy, it can be difficult to know where your personal data is syncing to your device, and vice versa.

3. **Many employees don't understand encryption -** Much of this flagged activity is due to users who don't know that most of these sites are not encrypted, or understand how to encrypt their data before putting it on the cloud.

4. **Natural turnover** - Even in stable organizations where employees are generally happy, turnover rates mean that it's difficult to instill lasting, cultural best practices around the use of these kinds of tools. What's more, technology is advancing at a rate that makes it difficult to educate employees on the latest tools, how they work, and potential data security dangers.

A PROACTIVE APPROACH

Companies need to educate users on what cloud sharing websites do and don't do to protect the data stored on them. Make it clear that these websites do not always encrypt information, and teach employees never to use the public share link unless they're dealing with information that is suitable for public consumption. Some organizations have had success blocking certain cloud sites, minimizing the attack surface and funneling all employee use to one tool that they can monitor appropriately and provide education. But, once again, this is another example of the importance of the ability to detect the "unknown unknowns." Organizations must be able to answer the important questions – like, "Are my employees properly using cloud sharing sites?"

A FEW EXAMPLES OF THE TYPES OF DATA FOUND PUBLICLY ACCESSIBLE ONLINE:

- Sensitive employee data
- Sensitive client data
- Legal info pertaining to social security, date of birth, and more
- Company financial information, including bank username/passwords
- Legal documents with signatures/logos/stamps
- Internal process mapping
- Company security plans
- Emails that can be used for phishing

"A DISPROPORTIONATELY HIGH VOLUME OF PHISHING ATTACKS USED LURES ASSOCIATED WITH DROPBOX, WITH TWICE AS MANY MESSAGES USING THE FILE-SHARING SERVICE TO ENTICE VICTIMS THAN THE NEXT MOST POPULAR LURE."

(The Human Factor 2018 Report, Proofpoint)

Companies who don't have clear policies around file sharing sites tend to have more phishing incidents, since phishing emails mimic alerts from popular cloud sharing sites.

HIGH RISK DATA TRANSFER

An all-too-common risk spurred by ill-defined guidelines.

USB storage devices are becoming less prevalent as cloud storage grows in popularity, but they're still a significant vulnerability for most organizations. 90% of Dtex assessments found employees putting data onto unsecured USB drives.

This poses a problem for a few reasons. Firstly, it opens the door to data leakage. Employees often use USBs for both personal and company use, which means that accidental data loss becomes much more likely as company data comes into contact with personal data and devices.

What's more, employees almost always use unencrypted USB devices, which means that losing the physical device could have dire consequences. And that's easy to do – who hasn't lost a USB device at one point or another?

of assessments found company data being transferred to unencrypted USB devices.

This is a

5% DECREASE

from last year.

HOW TO ADDRESS THE THREAT

Even if there's no malicious intent whatsoever, it's very easy to lose track of company data with USB drives. Unencrypted devices leave sensitive data unshielded from the world.

Organizations can mitigate some of this risk by providing encrypted USBs to employees that need them, which will be strictly for work use. Companies that want to take this control a step further can think about blocking USB activity, but also need to remember that blocking alone is never a catch-all solution. Companies must be sure that their security posture is prepared to find when things slip through the cracks.

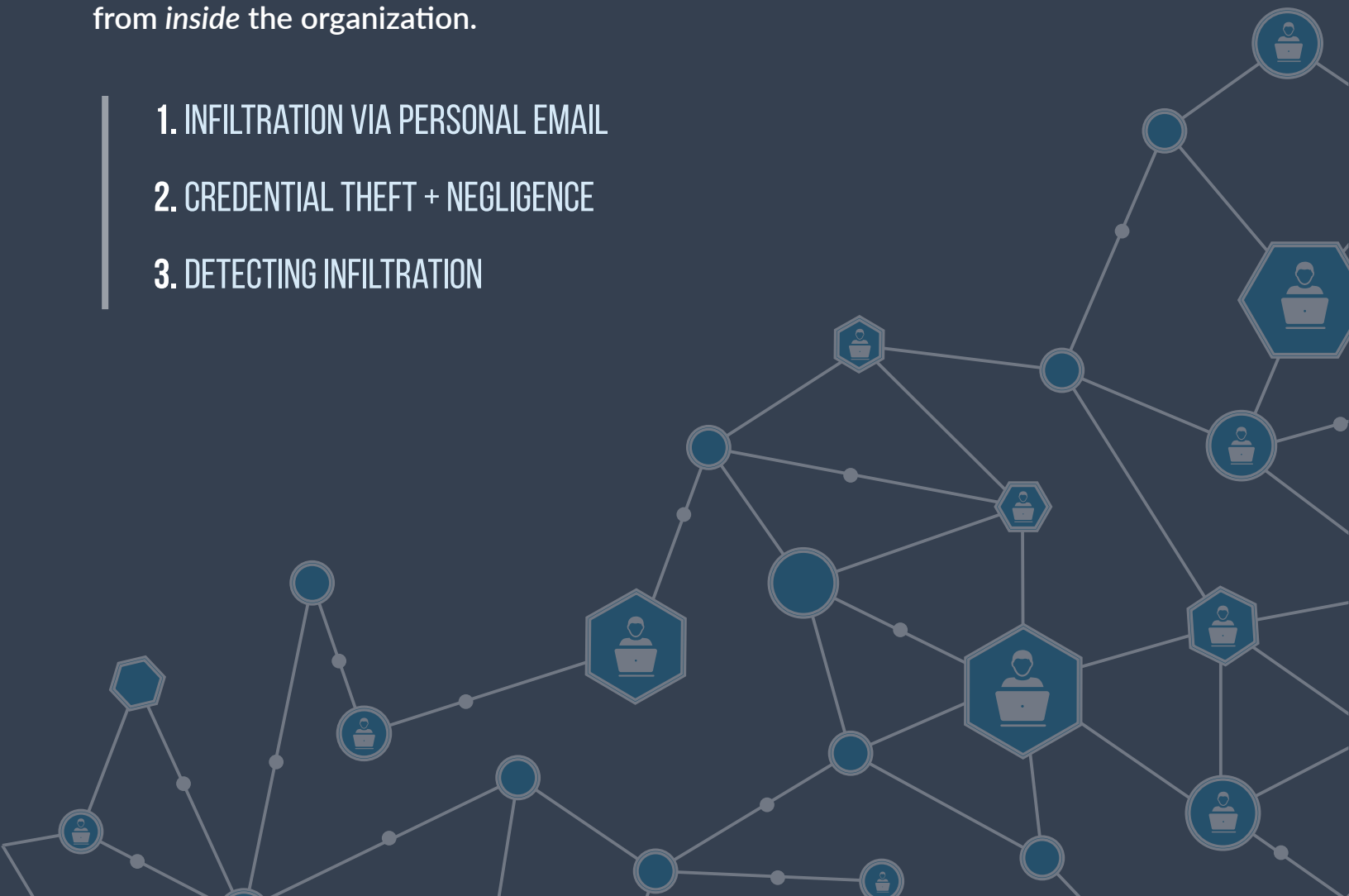
We often recommend to our clients a "Trust but Verify" approach. Many organizations want to provide their employees with the ability to do their jobs as freely as possible. By offering those privileges, but also making sure they have the visibility to confirm the way employees use them, security teams can see their risks and adjust policies accordingly.

PART THREE

INFILTRATORS

While not everyone thinks of if this way, outside infiltration absolutely qualifies as a form of insider threat. Like employees, infiltrators threaten organizations from within. And to strengthen the insider link, infiltration activity is also frequently a direct or indirect result of insider activity. Lastly, and most importantly, catching infiltrators is still a matter of seeing and understanding abnormal user behavior from *inside* the organization.

1. INFILTRATION VIA PERSONAL EMAIL
2. CREDENTIAL THEFT + NEGLIGENCE
3. DETECTING INFILTRATION



INFILTRATION VIA PERSONAL EMAIL

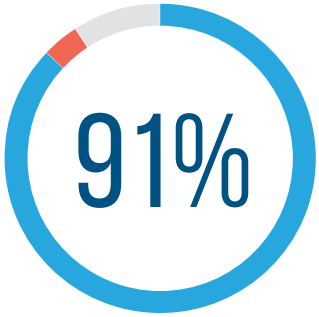
The easiest way to catch a Phish.

One of the most common ways that infiltrators get into an organization is through phishing attempts. Most frequently, these phishing attempts enter the organization through personal email accounts.

It's much easier for outside attackers to get in to the organization through a personal webmail account, because it avoids the security measures that are frequently in place on company email accounts. While some personal email services, like Gmail, have relatively sophisticated security measures built-in, others – such as Hotmail – are not nearly as fool-hardy. While phishing emails can, and do, make it past organizational security measures as well, personal email usage undeniably makes it easier for them to get into the corporate network.

Dtex assessments saw a slight increase in personal webmail activity this year – often even in organizations that thought they were blocking personal webmail usage.

However, the biggest phishing incident that we saw this year went through corporate email:



of assessments found employees using personal email on company machines, opening up a common avenue for phishing.

This is a

4% INCREASE

from last year.

REAL WORLD SPOTLIGHT: WHEN EMAIL SECURITY FAILS

On two dates, Dtex detected a customer's employees receiving a wave of phishing emails. Some of these emails contained malicious attachments that, when opened, spawned non-user-initiated activities. Other emails contained links in the email body pointing users directly to a malicious URL, which was flagged by one of the company's firewall products. It was an invoice-themed email, which pretended to contain an invoice for the company.

All-in-all, this email was a relatively "easy" phishing email – which is to say, for users who are even moderately familiar with phishing emails, it was not particularly convincing. However, in this situation, employees exhibited inconsistent ability to recognize the email as suspicious. Some opened the attachment, some clicked the link, and some forwarded the email to colleagues, who then opened the attachment or URL.

> **30% OF PHISHING EMAILS ARE OPENED BY THEIR INTENDED TARGET, AND 12% OF THOSE USERS CLICK THE MALICIOUS LINK OR ATTACHMENT.**
>
> *(2018 Verizon Data Breach Investigations Report)*

This email was fairly typical of invoice-themed attacks, so Dtex's analysts were suspicious of why the email had not been filtered out before it reached employee inboxes. It turned out that the company's inbound mail filter was not working during the two days that these emails were received, which is why they got as far as they did.

Thankfully, Dtex caught the problem before it became too widespread throughout the organization, but it serves as an important reminder of the importance of a defense-in-depth strategy. On any other day, the inbound mail filter would have stopped these emails from reaching inboxes – but it turned out to be critical that the company had another way to see what slipped through the cracks.

What's more, this incident proved that the organization needed to spend some more time educating users on how to identify suspicious email, and establish proper protocol for flagging them. This is something that all organizations need to do regularly, especially since infiltrators thrive on ignorant or ill-trained employees.

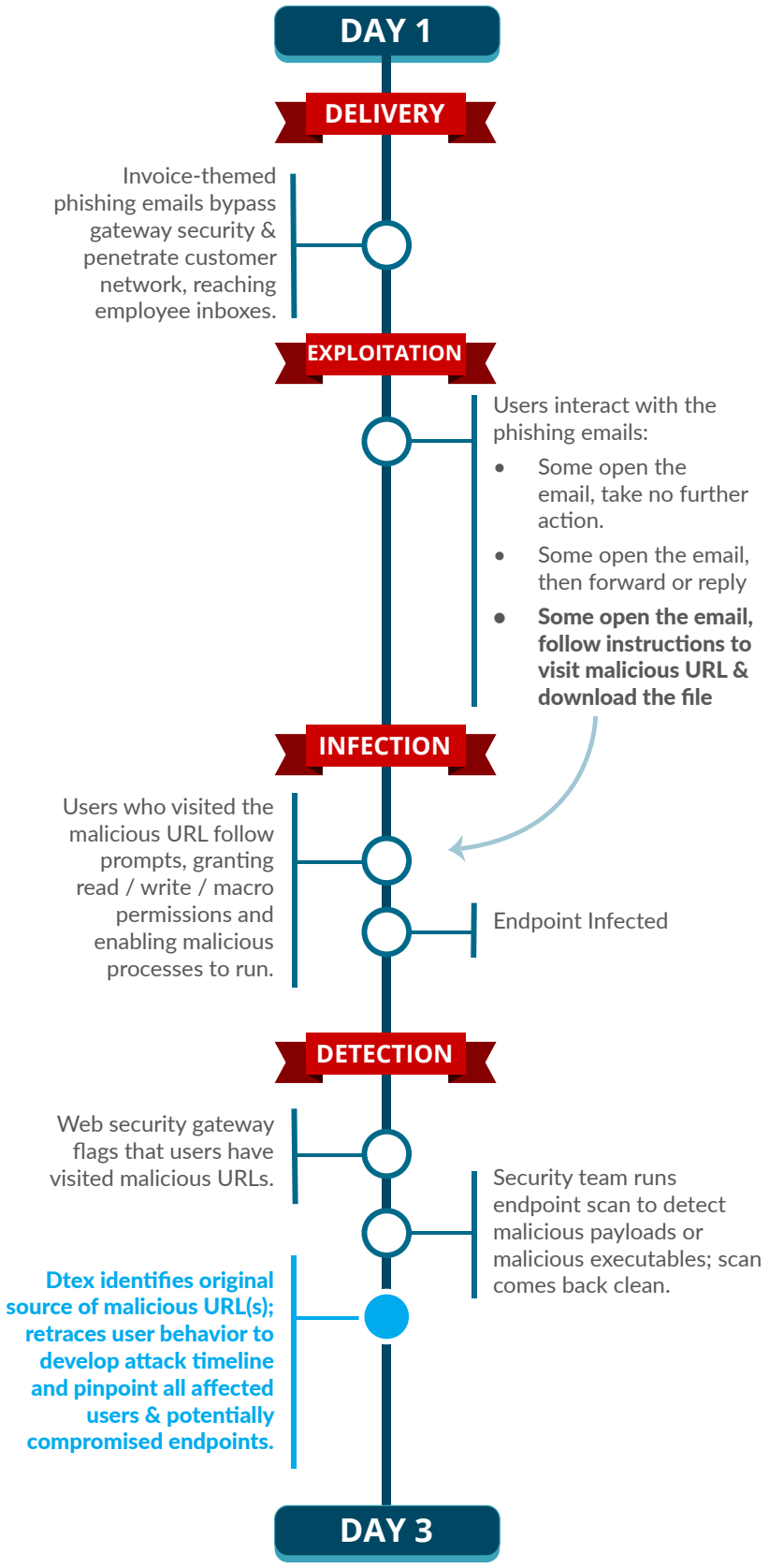
Ultimately, even in situations like this one that involve outside attackers, it all comes down to human behavior. Without Dtex, the customer would not have been able to see how their employees interacted with this phishing email after their other security measures failed. But by utilizing user visibility, they were able to quickly understand and mitigate the situation.

76% OF BUSINESSES REPORTED BEING A VICTIM OF A PHISHING ATTACK IN THE PAST YEAR.

Wombat Security, "State of the Phish Report"

SPOTLIGHT INCIDENT TIMELINE

Phishing Attack Progression, Detection, & Remediation



CREDENTIAL THEFT + NEGLIGENCE

A human problem, from the outside and the inside.

Credential theft is another risk that is also often based in user negligence. Not *all* credential theft is the result of an employee mistake – but those mistakes do make stealing data significantly easier. This year, Dtex caught employees jeopardizing credentials in a variety of ways that can expose users to credential theft, including:

- **Dormant User Accounts –** Assessments found that often, accounts that are supposed to be shut down completely are still active, vastly broadening the attack surface for potential credential thieves.
- **Outsourcing –** More and more organizations are outsourcing sectors of the business with administrative users, opening up those admin privileges to theft or misuse, since the organization cannot impose or verify security measures on credentials at an outside company.
- **Poor Execution –** In multiple cases, Dtex revealed that users were executing administrative commands in ways that expose usernames and passwords. These credentials could be exposed and identified by hackers with even basic skills, since they were so poorly protected.
- **Publicly Accessible Data –** Publicly accessible data has already been pinpointed as one of the biggest and most common problems faced by organizations this year. In some cases, the data includes credentials, completely open for theft or misuse:

> ASSESSMENTS FOUND THAT OFTEN, ADMINISTRATIVE ACCOUNTS THAT WERE SUPPOSED TO BE SHUT DOWN WERE STILL ACTIVE, OPENING THE ORGANIZATION UP TO CREDENTIAL THEFT RISK.

REAL WORLD SPOTLIGHT: EXPOSED CREDENTIALS

An assessment revealed a publicly accessible URL that led to a spreadsheet that contained credentials to different financial websites used by the organization. Anyone with these credentials would have full, unrestricted access to company bank accounts and other critical financial accounts – meaning that if they fell into the wrong hands, someone could easily steal huge amounts of money. These credentials were completely publicly accessible, and no one had any idea that they were exposed until it was detected in a Dtex User Threat Assessment – at which point, the documents were quickly pulled off of Google Drive.

DETECTING INFILTRATION

Know the signs to find.

Detecting infiltration is a matter of finding unusual user activity within the organization. Since credential thieves and other infiltrators hijack the accounts of normal users, detecting their presence is a matter of pinpointing wildly unusual behavior from that particular account. Here are a few signs that Dtex analysts have used to detect outside infiltrators:

ACTIVITY DURING UNUSUAL HOURS

When a user is active during extremely unusual hours – for example, in the middle of the night – that's a sign that something may be amiss.

UNUSUAL PRIVILEGE ESCALATION

Infiltrators will often do what they can to escalate the privileges of their chosen accounts, in order to increase their access and potential damage.

ABNORMAL AGGREGATION OF FILES

If an infiltrator is attempting to steal files, one of their first steps will be to seek out where sensitive data "lives" on the network and then download and aggregate those files to one location. This is a sign that security teams should be watching for regardless, since internal data thieves will nearly always take this step as well.

UNUSUAL USE OF HACKING OR LATERAL MOVEMENT TOOLS

For maximum damage, infiltrators will want to move laterally throughout the network, escalating privileges as they go. Typically, they will do this by using hacking or lateral movement tools, which oftentimes are not commonly used by the user whose accounts were stolen. By alerting on unusual use of these high risk tools, analysts can catch infiltration sooner.

UNUSUAL USE OF NETWORK ENUMERATION TOOLS

Infiltrators will often use network enumeration tools like Nmap or N-Stealth to investigate their environment. These tools will allow them to answer questions like, "Is the user/device that I'm on an admin account?" or, "What network shares can I access?" Gaining this information will allow them to spread throughout the organization and take advantage of their position more effectively.

ARE YOU PREPARED TO CATCH THESE WARNING SIGNS?

Many of these activities would not be detected without a source of high-fidelity user behavior data. We see many organizations miss critical warning signs because their security tools are attempting to reverse-engineer this visibility from log files, and aren't providing targeted user visibility – or their data is so noisy that their security team isn't seeing the signals that really matter.

PART FOUR

THE SOLUTION

There are many solutions that claim to “fix” insider threat, but if there’s one clear takeaway after investigating these types of user threats for so long, it’s that no single out-of-the-box solution can ever solve the insider threat problem in one fell swoop. User behavior isn’t black and white, and when that behavior is happening from within the organization, it makes things even more complicated. In order to address insider threats, organizations need to think holistically.

A SUSTAINABLE APPROACH

Organizations need to combat challenges with knowledge.

So, when there's no one bulletproof solution, how should organizations approach insider threat protection? Even in organizations that spend millions on cybersecurity, insider threats still slip through the cracks. Traditional security tools are failing to catch these risks. Ultimately, strengthening organizations against these types of threats requires a holistic shift in thinking.

CHALLENGES

The first step to developing an effective solution is facing challenges head-on. Regardless of varying size, industry, and location, many of the organizations we talk to are facing universal struggles:

Visibility: As this report has shown, threats can come from anywhere and anyone – IT admins, infiltrators who invade through a phishing email, or employees typically regarded as low risk like marketing employees. Many security tools require organizations to know what they're looking for in order to work effectively, like rule-based DLP products. But when it comes to insiders, these threats can come from anyone. When security teams need to build a rule to catch every type of threat, how can they possibly protect against the unknown unknowns?

Noise: On the other side of the coin, an overabundance of alerts is equally useless, especially if tools are alerting based on incomplete or ineffective data (like reverse-engineered log data). High false positives and overwhelming noise completely reduce the effectiveness of any security system.

Scalability: It doesn't matter how good a security tool is if it doesn't work. Organizations are increasingly discarding heavy solutions that are difficult to deploy across the entire organization, especially if they need to disable critical features just to make the tool usable at scale.

Privacy: For companies that do business in the EU, this is non-negotiable with the enforcement of GDPR looming. But even in less heavily-regulated countries, no one can afford to ignore privacy anymore, especially as employees become less tolerant of surveillance measures.

> **ACROSS THE BOARD, REGARDLESS OF COUNTRY, SIZE, OR INDUSTRY, WE SEE ORGANIZATIONS STRUGGLING WITH DATA QUALITY, NOISE, SCALABILITY, AND PRIVACY... AND FIGHTING THOSE CHALLENGES IS CRITICAL.**

THE COMPLICATED INSIDER THREAT LANDSCAPE

As insider threats become an emerging focus, security tools are still struggling to evolve. Security teams find themselves facing a complicated and sometimes frustrating solution landscape. While traditional security tools have their benefits, they're also facing consistent challenges.

SECURITY TOOL	BENEFITS	CHALLENGES
Security Information and Event Management (SIEM) *Software that collects and aggregates log data from existing IT infrastructure for analysis.*	» Highlights anomalies and trends from existing IT tools, providing some visibility into potential security issues » Can act as a single pane of glass to collate multiple data sources	» An incomplete data source; does not have the necessary visibility to detect user-based threats on its own. » Often very noisy and difficult to tune.
User Behavior Analytics *Analytics that reverse-engineer user behavior insights from log data.*	» Takes into account the fluidity of human behavior. » Adaptable	» Slow; takes a very long time to tune and see value. » Only as good as their data source, which is often flawed.
Data Loss Prevention *Rule-based tools that control what data users can transfer, and how, often through blocking.*	» Necessary for companies that need to hard-block certain activities under blanket company-wide circumstances.	» Rule-based – which means you only can catch what you know to look for. » No way to see what slips through the cracks (and things will slip through the cracks.)
Employee Monitoring *Tools that monitor user behavior, often through measures like keylogging, videos, screenshots, etc.*	» Provides a high degree of information into user behavior on an individual level. » Useful in litigation.	» Many use highly invasive measures like kelogging, screenshots, etc. » Will likely be seen as a privacy violation by employees; illegal in parts of the world. » Very heavy and difficult to scale.
User Behavior Intelligence (Dtex) *User behavior visibility specifically for the purposes of detecting insider threat, combined with patterns of known-bad behavior and adaptive analysts for insider threat detection.*	» Endpoint user behavior data provides human-readable contextual information. » Collects metadata – lightweight, scalable, & privacy-conscious. » Alert stacking & analytics reduce false positives; quick time to value.	» Highly tailored to insider threat detection – not intended for blocking or malware.

As proven throughout this report, Dtex regularly catches critical threats even in organizations where the traditional security tools above were already deployed. While all of these tools have their benefits, their flaws and blind spots mean that none of them can be a single solution against insider threats. Ultimately, in order to detect and stop user-based threats from within the organization, companies need a solution based on intelligence.

THE RIGHT VISIBILITY IS CRUCIAL

Security teams can't make any informed decisions until they know what's actually happening within the enterprise. And it's important to realize that not all forms of visibility are equal. Network-based data is not enough – not when so much of today's workplace activity takes place outside of the corporate perimeter, as employees do things like work from home or coffee shops, upload data to the cloud, etc.

What's more, we increasingly see organizations ripping out solutions that attempt to reverse-engineer insights from existing noisy, log-based data. This log data wasn't created for the purpose of finding insider threats. No matter how good the analytics placed on top of them are, they will still have critical gaps, and are often prohibitively noisy and slow to provide insights.

The cornerstone of any successful insider threat program is endpoint-based, user-based visibility that captures the right information – meaning, it captures behavior data that's explicitly intended to catch insider threats. What's more, insider threat programs need to build upon that data with intelligence that cuts down on noise and reveals insights, highlighting the abnormalities and suspicious behavior that teams really need to pay attention to.

PROTECTING EVERYTHING IS PROTECTING NOTHING

We observed a significant mental shift among security teams this year. More and more are realizing that it's impossible to create an air-tight security program that equally protects literally every facet of the organization's digital footprint. Attempting to protect everything in this way is essentially protecting nothing, because it's a losing battle and an unrealistic goal.

Instead, we're seeing the most forward-thinking teams pursue a more holistic approach. Many of our customers use the visibility provided by Dtex to reveal the most permeable parts of their enterprise. Once they can see the "hot spots" where data is seeing that most risk – like where it comes into contact with the greatest number of hands, where it's being transferred insecurely, etc. – they can then prioritize their security program to focus on those areas first.

This data driven, holistic approach to insider threat protection enables them to make the most impact with their resources.

THE KEY COMBINATION TO FIGHT INSIDER THREATS IS THE RIGHT VISIBILITY, ADAPTABLE INTELLIGENCE, AND AN INVESTMENT IN CREATING A CULTURAL ATMOSPHERE OF TRUST AND PERSONAL RESPONSIBILITY.

INVEST IN CREATING A CULTURAL SHIFT

The introduction of this report mentioned the somewhat concerning findings of our recent *Uncovering the Gaps* report, which revealed that a large number of employees don't feel a strong sense of personal responsibility for cybersecurity. This is a trend that Dtex analysts saw echoed throughout the year. As we've shown, the greatest security risks assessments found were the result of employees being careless, taking shortcuts, or simply being uninformed about their actions – often because they trusted the organization to protect them ("This email might be suspicious, but I'm sure that my computer has anti-virus software that will protect me if I open it…").

As technology advances and opens the enterprise up to more and more risks, it is critical that security teams work with HR and the entire organization to shift cultural attitudes about security. This will never happen overnight, but it's a non-negotiable investment in the long term security health of the company.

A good place to start would be to create simple, straightforward, and easily-readable security protocols and be certain that every employee is aware of them. Security teams and HR can then use that visibility to seize upon educational opportunities as they arise. Long-term, however, the goal needs to be to show employees that security is everyone's responsibility, not just the IT team's – and be prepared to verify their behavior.

In today's world, corporations will never be able to completely eliminate all risk. But by taking a high-level view of what's really happening in their organization and prioritizing the areas of the highest data loss risk, security teams can proactively tighten security where data faces the greatest amount of exposure.

GET YOUR USER THREAT ASSESSMENT

Are you ready to see how your company stacks up against these findings? A User Threat Assessment is quick and easy to set up, and Dtex is so lightweight that it has no noticeable network impact. At the end of the assessment, you'll receive a clear, prioritized report showing you exactly what your other security tools are missing.

Contact Us: info@dtexsystems.com

Phone: +1 (408) 418 – 3786

ABOUT THIS REPORT

Background and Demographics

ABOUT THIS REPORT

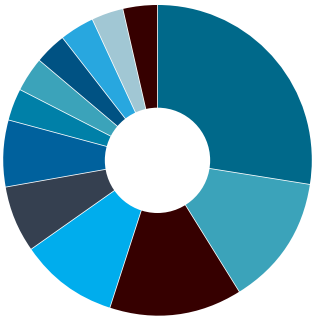
The 2018 Insider Threat Intelligence Report data was drawn from the User Threat Assessments conducted on Dtex customers and prospective customers around the world.

These organizations spanned a wide variety of countries and industries, and ranged in size from midsize businesses to large multinational corporations.

ABOUT DTEX SYSTEMS

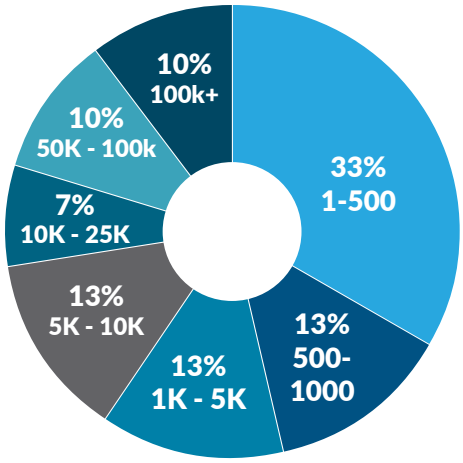
Dtex Systems arms enterprises across the globe with revolutionary technology to protect against user threats, data breaches, and outsider infiltration. As the only solution combining unparalleled endpoint visibility with advanced analytics, Dtex is able to pinpoint threats with greater accuracy than traditional security methods without adversely impacting user productivity. To learn more, visit www.dtexsystems.com.

DISTRIBUTION BY INDUSTRY

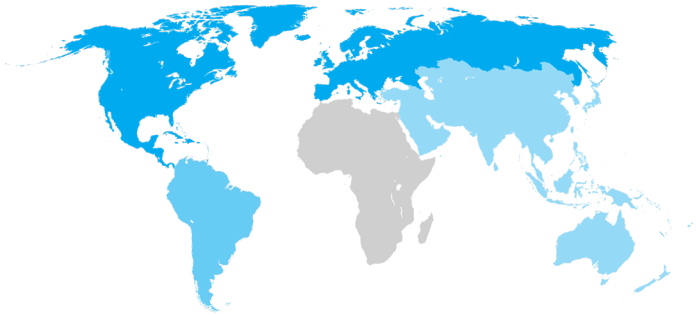


Financial	26%
Law	13%
Technology	13%
Public Sector	10%
Energy	7%
Retail	7%
Transportation	3%
Real Estate	3%
Pharmaceutical	3%
Manufacturing	3%
Food & Beverages	3%
Business Services	3%

DISTRIBUTION BY NUMBER OF EMPLOYEES



DISTRIBUTION BY HQ LOCATION



Europe	37%
North America	30%
South America	23%
Asia/Pacific	10%