2017 INSIDER THREAT INTELLIGENCE REPORT

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

Introduction

2017 INSIDER THREAT INTELLIGENCE REPORT

Big companies, small companies, healthcare, finance, entertainment, media, law....The specifics may vary, but the big picture is the same: your data is insecure. With today's technology, it's becoming more difficult and time consuming to proof your internal systems against day-to-day user behavior.

According to the Cybersecurity Market Report, spending on cyber security is expected to top $1 trillion from 2017 to 2021. Yet, companies are still facing crippling data breaches due to sensitive data leakage and exfiltration. Why are we seeing this rise in data breaches despite increased investment? The answer lies with your users.

THE IDENTITY THEFT RESOURCE CENTER (ITRC) REPORTS THAT THERE WERE MORE THAN 980 DATA BREACHES RECORDED IN 2016, RESULTING IN MORE THAN 35 MILLION RECORDS EXPOSED.

Over the past few years, we have seen a fundamental change in how people – and businesses – use technology. Every year, distributed enterprises, remote workforces, and bring-your-own-device policies become a more expected everyday reality.

Today, too many people immediately take the term "insider threat" to mean something very specific: images of shady, hoodie-clad employees hacking the corporate network late at night. Although intentional insider theft is far from unheard of, the insider security threat is a bigger, broader problem. In the real world, we find that user-based security incidents fall into three general groups:

MALICIOUS USERS

Users who intentionally harm the company. Most frequently, these are employees who steal sensitive data, intellectual property, client lists, etc. They can also be disgruntled saboteurs.

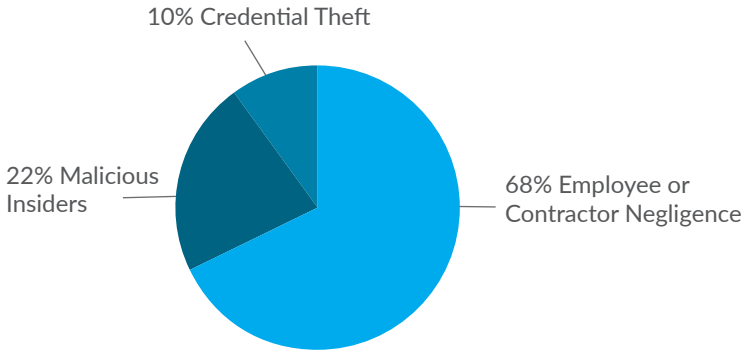
NEGLIGENT USERS

Users who cause security breaches by accident. Many companies underestimate this group. These users unintentionally risk security by attempting to find more convenient solutions, a misunderstanding of security practices, or human error.

INFILTRATORS

Outside attackers who infiltrate your organizations. This includes hackers, ransomware, credential thieves, etc. We consider these to still be "insiders" because, for all intents and purposes, they are acting as an insider within your organization – and catching them requires the same tools and strategies.

Last year, we partnered with the Ponemon Institute to research the 2016 Costs of Insider Threats Report. For that report, Ponemon analyzed 874 insider incidents and found that they broke down as...



Gartner analysts predict that by 2018, 25% of corporate data will completely bypass perimeter security and flow directly from mobile devices to the cloud. These changes in the way we interact with data are forcing CISOs to approach security differently. Security executives are increasingly finding that user driven technologies like mobile devices and cloud services present a major barrier to traditional data breach prevention and response strategies. So while our users are evolving, our approach to monitoring the risk within the enterprise has not.

> ACCORDING TO THE 2015 VERIZON DATA BREACH INVESTIGATION REPORT, PEOPLE ARE THE COMMON ROOT CAUSE IN 90 PERCENT OF TOTAL SECURITY INCIDENTS THAT RESULT IN DATA BREACHES.

THE PATH FORWARD

Perimeter-based security approaches simply don't work anymore. Technology is moving so quickly – and users are becoming so savvy – that you can no longer count on restricting employees with lock-and-block techniques.

In a world where the user cannot be contained, the ability to gain visibility into user behavior, while respecting user privacy, is critical in order to see your next generation risks. Users themselves can be both the greatest liability as well as asset in building a culture of data responsibility, transparency and accountability.

ABOUT THE DTEX INSIDER THREAT INTELLIGENCE REPORT

Dtex conducts regular insider threat assessments across a diverse customer base. Using a unique combination of endpoint visibility, user anonymization, analytics, and expert insight, we're able to identify major insider threat risks that other tools can't see. Our solution, our decade of experience in working with companies on User Behavior Intelligence, and our global footprint allow us to see unique insights into emerging user behavior patterns – both on and off corporate networks.

This report is our second release of the Dtex Insider Threat Intelligence Report – an initiative started in 2015 to track, analyze, and share the impact of human behavior on enterprises of all sizes and industries.

2016 Assessment Top Takeaways

REPORT HIGHLIGHTS

Dtex analyzed 2016 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. These were the top takeaways from the report:

HIGH RISK APPLICATIONS

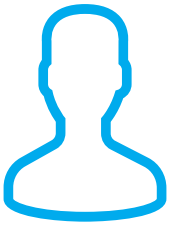
95% of companies saw staff researching, installing or executing security or vulnerability testing tools. The use of high-risk applications continues to pose an increasing threat to enterprises.

PUBLIC DATA

64% of companies found publicly accessible corporate information on the web. Sensitive data is frequently available via the public web – mostly because users share information in unsecure ways.

SECURITY BYPASS

Usage of anonymous web browsers and anonymous VPN doubled from 2015 to 2016. More and more employees bypass security, particularly through the virtual private networks and hacking tools.



LEAVERS & JOINERS

56% of organizations had potential data theft by leaving or joining employees. Employees who are leaving or joining the company pose the highest data theft risk.

INAPPROPRIATE INTERNET USAGE

59% of companies saw inappropriate Internet usage. Inappropriate internet usage, like pornography and gambling, is a key indicator for other high risk behavior.

PART ONE

MALICIOUS USERS

Malicious users are the “insider threat” as most people think of it: an employee intentionally trying to steal data or harm the company. Catching these insiders goes beyond simply looking for data exfiltration – though that is a big part of it. These are users who have an intentional plan, and may in some cases be super users or admins with special privileges. In order to catch them before the damage is done, enterprises need to be aware of the other signs of ill intent.

1. SECURITY BYPASS AND HIGH RISK APPLICATIONS
2. DATA THEFT VIA PERSONAL EMAIL
3. LEAVERS AND JOINERS
4. INAPPROPRIATE INTERNET USAGE
5. PIRATED SOFTWARE AND MEDIA

Insiders are Turning Security Inside Out

SECURITY BYPASS

95%

of assessments discovered staff researching, installing, or executing security or vulnerability testing tools.

Usage of anonymous web browsers and anonymous VPN

DOUBLED

from 2015 to 2016.

An overwhelming amount of our data has found that security bypass is the first step towards data theft or other destructive behavior. This includes the use of vulnerability testing or hacking tools (like Metasploit), anonymous web browsers (like TOR), or anonymous VPN tools.

Tools like this are becoming increasingly common among everyday users. The Global Web Index estimates that more than half a billion people **(24% of the world's internet population)** have tried or are currently using anonymous VPN services.

When it comes to security bypass, our analysts have found that the common saying holds true: where there's smoke, there's a fire. If a User Threat Assessment uncovers use of the TOR (The Onion Router) browser, for example, it's highly likely that the user is trying very hard to cover their tracks. That level of obfuscation is a red flag that the user is engaging in prohibited – or potentially even illegal – activity.

Dtex analysts see similar findings when it comes to security bypass research. This is when an employee spends time clearly researching how to get around security measures, like running searches for terms like, "How to disable DLP" or "How to uninstall Dtex." We often find employees researching security bypass for hours on end – and they're extremely persistent. **Most of the time, these malicious employees only stop once they're caught.**

There are occasionally cases where employee motivations for using more common privacy or obfuscation tools fall under shades of grey. Sometimes, employees use these tools because they're frustrated with the restrictions in their workplace and are just looking to save time by using their favorite file sharing platform or messaging tool.

However, even then, their circumvention ends up causing even more security problems. These services potentially allow others to use their internet connection for illegal activity – which can create an opening for malicious third parties to snoop into unencrypted company data. In fact, one of the most popular "free" VPN services actually sells users' bandwidth and IP address to the highest bidder – **potentially to be used for malicious cybercrime.**

WHERE SECURITY TEAMS GO WRONG

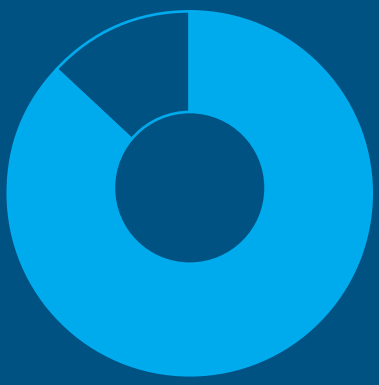
Many security teams focus solely on finding and stopping the specific malicious event itself – the specific act where a user steals data, commits sabotage, or engages in another malicious or prohibited activity. From there, security teams then have to build signatures and indicators of compromise based on that event. However, this method falls short when it comes to stopping unusual or never-before-seen attack – or, even more importantly, stopping an attack before it happens. In almost every case, it is easier to detect the suspicious activity leading up to an attack than it is to detect the attack itself. Security bypass is a common example. Dtex has stopped hundreds of potential attacks by flagging users attempting to circumvent security – an extremely common first-step to data theft.

REAL WORLD SPOTLIGHT: UNLIKELY HACKERS

When it comes to hacking tools, it is especially important to pay attention to the role and normal behavior of each user. At a large telecommunications company, a Dtex User Threat Assessment identified a marketing employee using a highly abnormal number of hacking tools while also doing a number of "how to" searches about hacking and security bypass. The assessment saw this user, over time, installing and learning how to use these high risk applications – and then caught him attempting low-level hacking attacks on other websites. After Dtex alerted the company to his behavior, it was revealed that the website he hacked belonged to a company that was currently undergoing a merger with the telecom enterprise, opening the company up to legal and financial risks. Thankfully, Dtex caught this behavior early, before any real damage had been inflicted. The customer's CISO informed the targeted company's CISO about the attempted attack, and was able to give them full details and background information. The offending employee was let go and escorted out of the company.

The simplest avenue out of the enterprise.

DATA THEFT VIA PERSONAL EMAIL



87%

of companies saw employees using personal web-based email on company endpoints – even though many of these companies had measures in place to block personal email providers.

It's an oversimplification to immediately equate personal email usage to malicious intent – a point we will revisit when we discuss negligent users. However, it is impossible to ignore the fact that personal email accounts (like Gmail, Yahoo, Hotmail, etc.) can absolutely be used as an avenue for data theft.

Simple sent emails, file attachments, or calendar entries are among the most obvious ways that an email account can be used to exfiltrate data. But the security community has seen much trickier methods, too. For example, users can use drafts to save and transfer information without leaving a network trail.

In 2014, hackers famously used Gmail drafts as a command and control feature, proving that webmail can be used in all sorts of unconventional ways to infiltrate an organization. All of this is especially worrisome when it's taking place off

REAL WORLD SPOTLIGHT: COLLUSION

A Dtex risk assessment uncovered that employees were colluding with an outside contractor who was bidding on a company job. Once the employees were made aware that Dtex was installed, they started using their personal networks instead of the corporate network. Since Dtex gets its visibility from the endpoint itself, their attempt to hide their behavior didn't work – but the story is a testament to the importance of endpoint visibility!

network, when the user is bypassing all corporate control – leaving you blind, with your hands tied.

Personal webmail can also be used to cover tracks and hide activity. We've seen webmail accounts used as a medium for collusion between malicious actors. In several cases, we caught multiple employees logging into the same webmail account to do things like share pirated media and applications, which is a proven way to seriously increase cybersecurity risk. Even worse, this method could also easily be used to maliciously share sensitive information without leaving a trail.

REAL WORLD SPOTLIGHT: THE SIDE HUSTLE

At one multinational customer, Dtex caught an employee illegally selling company property. Each day, this employee would open a personal email account in Chrome's Incognito Mode – an obvious attempt as obfuscation – and use that personal email account to run a business. Ultimately, it was discovered that this employee was illegally selling company property, as well as engaging in other prohibited activity such as gambling and porn. Dtex worked with the company's internal forensics team to collect evidence against this employee that was ultimately used in legal prosecution.

> USERS CAN USE DRAFTS TO SAVE AND TRANSFER INFORMATION WITHOUT LEAVING A NETWORK TRAIL.

The revolving door of data theft hits you on the way in and the way out.

LEAVERS AND JOINERS.

56%

of organizations assessed had potential data theft by leaving or joining employees.

Leavers tended to show abnormal file aggregation detected in the

LAST 2 WEEKS

of employment

Joiners tended to import large amounts of data in the

FIRST 2 WEEKS

of employment

Most people already know that employees are riskiest when they're about to leave the company. Everyone has heard the stories of product managers who steal proprietary plans, engineers who sneak out valuable code, or salespeople who poach critical client lists. Our own assessments have shown that more than half of organizations had this problem.

A recent report found **93 percent of employees admit to engaging in at least one form of poor data security,** and reported that 23 percent of respondents admitted they would take data from their company if it would benefit them. Other research has shown that after leaving a company, 89 percent of employees still have access to at least one application or to proprietary corporate data. In some of the worst cases we've seen, organizations have even lost their patent or trademark rights.

However, while leaving employees are a pervasive security risk, it's also important not to forget about joiners – new hires joining your organization.

> 23% OF RESPONDENTS IN A RECENT STUDY SAID THEY WOULD TAKE DATA FROM THEIR COMPANY IF IT WOULD BENEFIT THEM.

Oftentimes, no one gives new hires a second glance. However, it is surprisingly common that new hires bring stolen data into a new organization. This is equally as troubling for a few reasons.

First of all, it's morally questionable to keep and use stolen data. Even Pepsi returned stolen secrets to their most bitter rival, Coca Cola.

Morality aside, it's legally dangerous. We've seen companies harshly burned for having stolen data in their network, and exposed to grave legal action.

What's more, there's another obvious threat: this employee most likely won't be working for your enterprise forever. If you find out they've brought stolen data into your network, they probably are going to take your data when they leave, too.

SPOTLIGHT:

REAL WORLD EXAMPLES

A CLOSE CALL

Dtex found an employee that was leaving a Finance company on good terms had transferred personal data as well as corporate data onto a USB from the laptop that was provided by the company. Because IT was able to promptly identify this risky user behavior, the employee was brought back on premise to remove the corporate data.

STOLEN CLIENTELE

At a large utility company, Dtex discovered that a prior employee had downloaded a large list of client contact information. Investigation revealed that this employee had deliberately stolen this client information to take to their new position at a competitor. Armed with Dtex's logs and context, the company was able to conduct a forensic investigation and pursue legal action.

Insiders are betting the company farm –and losing.

INAPPROPRIATE INTERNET USAGE

43%

of assessments discovered online gambling activity: lottery, sports betting and bitcoin-related activities.

59%

saw other inappropriate internet usage such as pornography.

The internet is a double-edged sword. It helps workers get things done faster, better, and more easily – but it also can be a massive distraction. Some of these distractions are mostly innocent, like social media, entertainment, shopping, etc. However, our risk assessments also frequently find totally inappropriate workplace activity, like gambling or pornography.

During our risk assessments, we've found that accessing porn and gambling sites on corporate devices is generally an indicator of employee negligence. **In companies that had employees engaging in this kind of unsavory behavior, we found overall risk scores that were three times higher than the norm.**

Furthermore, most employees need to circumvent security measures to access these websites – which means that they're weakening your overall security posture and you have no way of knowing when they do it.

> WE'VE FOUND THAT ACCESSING PORN AND GAMBLING SITES ON CORPORATE DEVICES IS GENERALLY AN INDICATOR OF EMPLOYEE NEGLIGENCE.

Employees sail away with Pirates booty...
Leaving their companies open to marauding attackers.

PIRATED SOFTWARE & MEDIA

76%

of assessments found staff using pirated software and media.

$$$

DAMAGES CAN BE AS HIGH AS

$150,000

PER PROGRAM COPIED.

Pirated software is a security threat in two major ways. Firstly, it is a legal vulnerability. Having pirated software in your enterprise opens you up to potential legal action in a variety of ways. The Business Software Alliance is a driving force behind thousands of investigations into these cases each year.

Beyond that, there's another big danger involved: **malware.** Pirated software downloaded from the internet is frequently packaged with malware or is malware in disguise. In a recent BSA Global Software Survey, **49% of CIOs identified security threats from malware as a major threat posed by unlicensed software.** Those same CIOs estimate that 15 percent of their employees load software on the network without their company's knowledge. Worst of all, **26% of employees actually admitted to installing outside software on work computers.**

PLUS...

the government can pursue a copyright infringement case against you. In the U.S., that can translate to fines up to $250,000, five years in jail, or both.

REAL WORLD SPOTLIGHT: ACCIDENTAL PIRATES

Media piracy can happen even when a user is not intentionally engaging in theft. In one case, a Dtex Risk Assessment detected that an employee was using company equipment to convert YouTube videos to mp3 files – a clear violation of piracy laws, and a big potential malware risk. Once the security team was made aware of this activity, they were able to stop and educate the employee before the activity resulted in fines or malware.

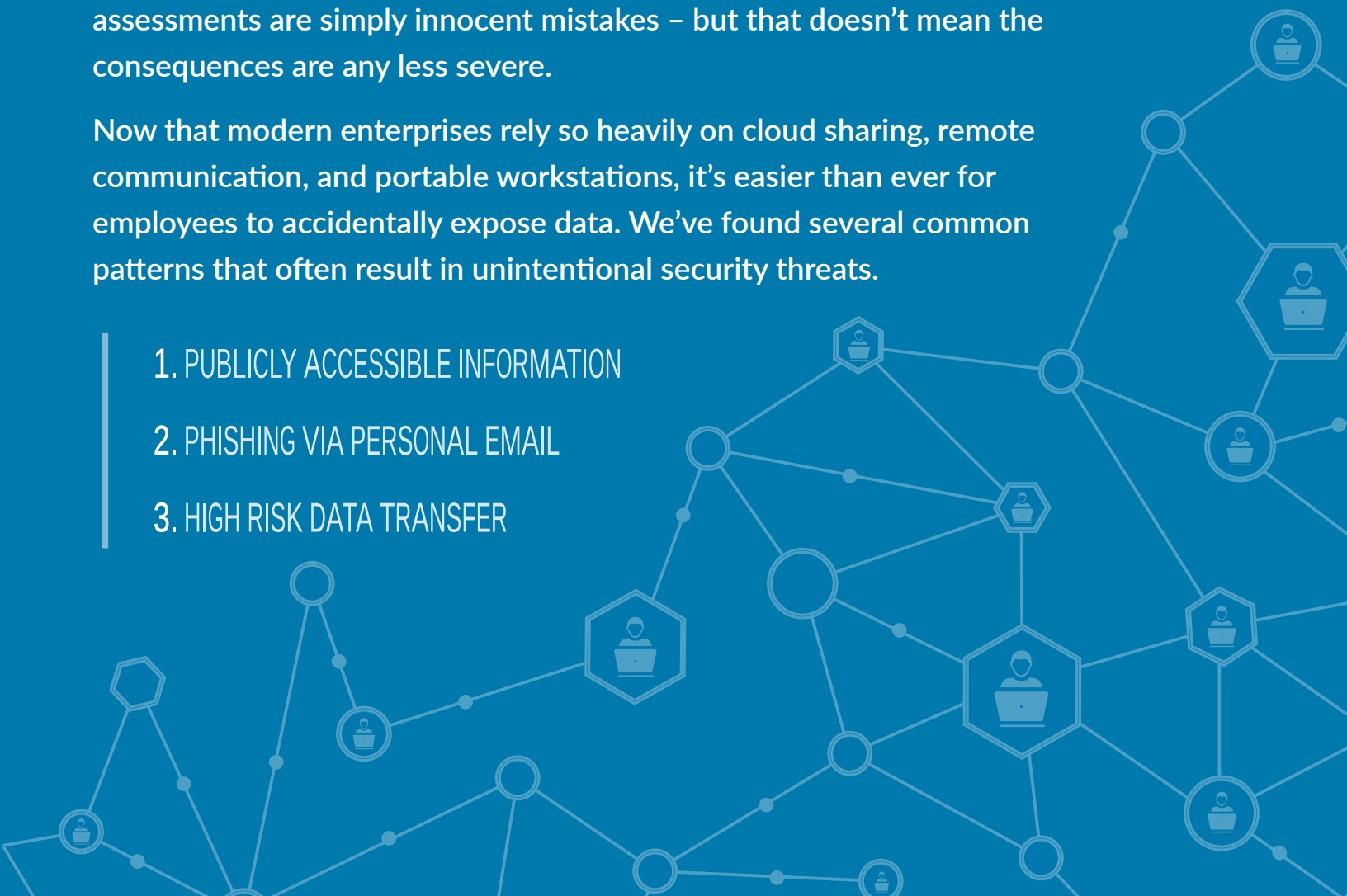
PART TWO

NEGLIGENT USERS

Many enterprises focus their security efforts on preventing intentional data theft. However, according to our study in conjunction with the Ponemon Institute, 68% of insider security incidents are attributed to employee negligence – not malicious intent. This supports what our analysts have personally seen in our User Threat Assessments, too. The vast majority of security risks that we uncover during assessments are simply innocent mistakes – but that doesn't mean the consequences are any less severe.

Now that modern enterprises rely so heavily on cloud sharing, remote communication, and portable workstations, it's easier than ever for employees to accidentally expose data. We've found several common patterns that often result in unintentional security threats.

1. PUBLICLY ACCESSIBLE INFORMATION
2. PHISHING VIA PERSONAL EMAIL
3. HIGH RISK DATA TRANSFER



Workforces are extending open invitations for data theft.

PUBLICLY ACCESSIBLE DATA

64%

of assessments found publically accessible corporate information on the web.

Nearly everything about today's workplaces is shifting rapidly, from technology to interaction to expected behavioral norms. This means that most organizations have many different people from many different places using an unmanageable number of tools to efficiently and conveniently share information.

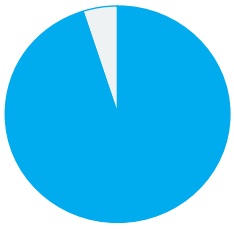
Our risk assessments frequently find that employees, contractors, and business partners often **unintentionally sacrifice security for the sake of connectivity and convenience.**

But here's what's especially alarming...According to a report by Skyhigh, **corporate use of cloud storage is reaching a truly shocking rate:**

ACCORDING TO A STUDY BY FIELDGLASS...

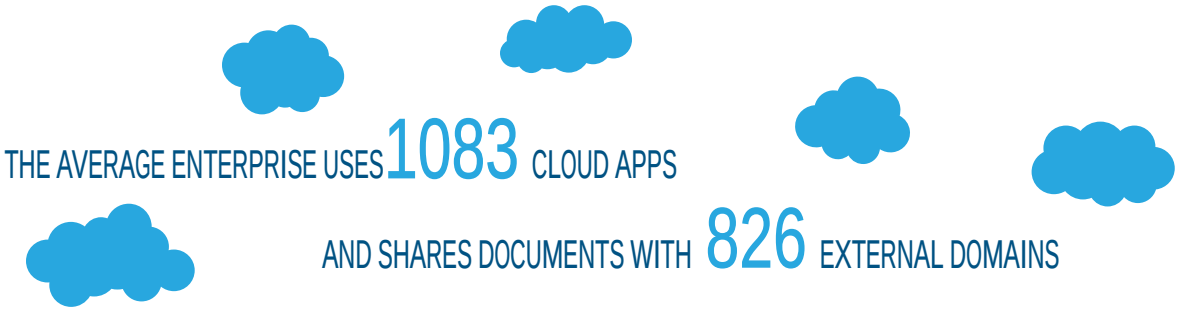
NEARLY 35 PERCENT

of today's total workforce is comprised of non-employee workers - which includes temps, freelancers, contractors and statement of work-based labor.



95 PERCENT

of organizations view a remote, distributed workforce as a key element to developing and running a successful business.



- *Skyhigh Cloud Adoption and Risk Report*

Of those documents, **6% are shared with personal email addresses like Gmail, Yahoo Mail, and Hotmail** – and even worse, **more than 2% are publicly accessible on the internet.**

In modern, distributed enterprises, **it's impractical to block all of these websites.** Not only are their numbers growing every day, making it nearly impossible to block every single one, but modern employees also need to be able to share and communicate easily to get their job done. However, security professionals need to master a balance – educate employees on safe use of cloud tools, block where necessary, and have visibility into what files are making it to the cloud insecurely.

REAL WORLD SPOTLIGHT: POORLY-KEPT SECRETS

One Dtex customer who needed strong physical security was in the process of moving to a new location. Dtex discovered that their architectural and security plans were **publicly accessible on a cloud storage website through the contractors that they were working with.** The physical security designs of this new location were so important that if they were compromised, the plan would have to be completely re-architected. Thankfully, Dtex revealed the problem early enough that the security team could verify that the plans had not been accessed and mitigate the problem before a breach occurred.

REAL WORLD SPOTLIGHT: THIRD-PARTY COMPROMISE

Yet another Dtex assessment found design plans **publicly accessible through a third party vendor's use of cloud storage.** Even in companies with strict security postures and Non-Disclosure Agreements, third party vendors and contractors still pose a significant risk for accidental data exposure. After discovering this vulnerability, this customer was able to **remove the publicly accessible data before it was breached, and modified their contractor policies to protect against this in the future.**

Insiders catch the big phish.

PHISHING VIA PERSONAL EMAIL

We have already addressed the dangers of personal email use when it came to data theft and malicious collusion. But perhaps the most common danger of personal email in the corporate environment is that it's an entry and exit point that you have little visibility into.

Personal webmail services are totally removed from the controlled environment of a company inbox, meaning that **they're far more susceptible to phishing attacks.** It bypasses all corporate controls, giving attackers an easy, unobstructed avenue into your organization's network. This is an even bigger risk off of the corporate network, where traditional monitoring and proxy methods are blind – especially in today's age of laptops and other portable work devices.

Even well-intentioned users pose a big risk through exposing the company to more threats by **opening or downloading an email that they shouldn't.** If an employee clicks on a phishing email while on the corporate network, exposing the entire company to a hacker or virus, the results could be catastrophic.

RECALL THAT **87%** OF DTEX RISK ASSESSMENTS FOUND EMPLOYEES USING PERSONAL EMAIL ON COMPANY ENDPOINTS.

REAL WORLD SPOTLIGHT: A PHISH IN DISGUISE

A phishing attack is rarely an isolated event. At a large financial institution, a Dtex User Threat Assessment flagged a publicly accessible cloud storage link and a long, suspicious .exe file. Upon closer review, Dtex analysts identified that a user had clicked on a phishing email through their personal webmail account. This company banned personal email on their corporate network, but had no way of blocking it when the endpoint was off-network.

This email was designed to look just like a DropBox share notificiation, with a link to a DropBox file that was an executable file disguised as a PDF. After downloading this file, the user was savvy enough to realize that it was suspicious and deleted it from their machine. However, by then, the virus had spread. Dtex saw this application create copies of itself in several different places on the user's machine, hiding itself. This malicious application was a never-before-seen variant, so it was not detected by the enterprise's anti-virus system.

With this information, the security team could quickly find and contain the virus. **If they hadn't had this level of visibility, the attack would have gone undetected – causing potentially catastrophic damage.**

Your data is in the cloud...whether you know it or not.

HIGH RISK DATA TRANSFER

95%

*of assessments found sensitive corporate data in **both the cloud and unencrypted USB devices.***

While data exfilrtration via USB has declined, the use of file sharing websites and applications has dramatically increased.

We considered "high risk transfers of corporate data" to mean any file transfer activity that was deemed high risk. That includes files with confidential file names, files stored in sensitive network locations, files with high risk file extensions, or any combination of the above. This also includes file transfers to unencrypted removable mass storage devices or online document storage and file sharing websites.

Ultimately, we found that **the vast majority of enterprises have sensitive data floating around somewhere it shouldn't be** – whether that be the internet or an unprotected device.

There are a few big dangers associated with this:

1. High-risk file sharing services could be hacked or breached, putting your precious data into the hands of unscrupulous criminals.
2. It is very easy to misuse the built-in sharing capabilities of these tools, even unintentionally – for example, it's easy to accidentally set a Google Doc to "public" instead of "private" if the user isn't familiar with the tool.

THE AVERAGE ENTERPRISE LEVERAGES:

PLUS, EACH AVERAGE EMPLOYEE USES:

Statistics from Skyhigh's Q4 2016 Cloud Adoption & Risk Report.

This problem isn't going to go away. In fact, a report from Skyhigh found that of all the files uploaded to file-sharing services, a whopping **16% contained highly sensitive – and oftentimes, regulated – data.** Even worse, **36% percent of documents stored within file sharing services are accessible to people beyond the user themselves.**

We hear CIOs and IT professionals regularly voice concerns over their ability to monitor data.

File transfer and online storage data is a big part of those fears – especially since they play a major role in maintaining security compliance requirements. Both from a regulatory and a security standpoint, **it is critical that security professionals are able to track where their data is going.**

SPOTLIGHT:

REAL WORLD EXAMPLES

FILE SHARING GONE WRONG

At a global technology manufacturer, Dtex discovered that schematics for a ready-to-mass-produce device were publicly accessible on a cloud storage site. It turned out that this was because employees were sharing data with contractors and vice versa in the most convenient way, unintentionally exposing critical data. After discovering this, the customer removed the schematics from the web and provided new guidelines for sharing practices for employees and contractors.

PART THREE

INFILTRATORS

We include infiltrators – like hackers, credential thieves, and ransomware – in our definition of "insider threat" because ultimately, infiltrators are taking advantage of vulernable insiders in order to gain access to your corporate network. Credential theft and negligent users, for example, often go hand in hand.

We have seen an increase in infiltration attacks, and they are the most difficult cases to detect using traditional security tools. Gone unchecked, even a single infiltrator can be devasting. In order to find and stop these threats, you need to employ the same understanding of user behavior that you need in order to detect negligent or malicious insiders.

1. INFILTRATION THROUGH PERSONAL EMAIL
2. USER NEGLIGENCE AND INFILTRATION
3. COMMON SIGNS OF INFILTRATION

Infiltrators are invading through simple mistakes.

INFILTRATION & NEGLIGENCE

Oftentimes, user negligence and infiltration go hand-in-hand. This can be through personal email, through poor security practices, or often, because employees don't know how to recognize suspicious applications or emails.

For example, one Dtex customer used local admin accounts on their network and endpoints. As time went on, **IT administrators would share the credentials to these admin accounts many times over** – but didn't regularly change the passwords. **Dtex was able to identify that many employees had access to these admin accounts.**

This particular customer was able to remedy the situation before an infiltrator could take advantage of it, but many other companies aren't as lucky. **Shared admin credentials like that are a goldmine for hackers.** For example, one of the many employees who had those admin credentials could have easily clicked on a phishing email while off the company network. Frequently, phishing emails will install malicious software that gives a third party remote access. Since this employee has admin access, the attack would be able to elevate their privileges and move laterally throughout the organization quickly and easily.

INFILTRATION THROUGH PERSONAL EMAIL

Earlier in this report, **we discussed the potential impacts of personal email usage in the hands of both malicious and negligent users.** Recall that 87% of our assessments revealed personal email use on corporate endpoints. Because of its pervasive use, **personal email accounts are a common entry-point for infiltrators and a prime target for credential theft.**

Today, the average user is inundated with online accounts and services. According to a study by Dashlane, **the average US person has 130 online accounts** -- and reuses their favorite passwords. Even worse, a frightening number of people have only one password that they use for every single website -- webmail accounts included. As of 2013, **55% of UK adults used ONE password for most, if not all, websites.** This means that too often, a hacker obtaining one set of credentials is actually obtaining all credentials. Worse, sometimes people go months, years, or forever without even knowing that their account was compromised, **opening up your endpoints and, by extension, your corporate networks to external attack.**

Follow the trail to the infiltration culprit.

COMMON SIGNS OF INFILTRATION

Hackers and external infiltrators almost always follow the insider threat kill chain – a sequence of activities that Dtex analysts have found in common across events from enterprises of all sizes and industries. Dtex analysts look for the following steps as red flags to infiltration:

RECONNAISSANCE. An infiltrator that recently gained access to the system will conduct an unusual number of searches, access atypical folders, etc. in order to gather intel.

PRIVILEGE ESCALATION. An infiltrator will almost always attempt to use any available administrative access to escalate their own stolen account's privileges and get increased access to the corporate network.

LATERAL MOVEMENT. The infiltrator will use their new privileges to move laterally throughout the organization.

DATA AGGREGATION. If the infiltrators goal is data theft or ransom, they will collect sensitive data in order to steal it from the corporate network.

Unfortunately, many enterprises are **unable to catch infiltrators before the damage is done.** Many Dtex customers rely on traditional technologies like Data Loss Prevention and User Behavior Analytics. These are helpful and important security measures, but **they don't go quite far enough to see and identify suspicious user behavior.** Data Loss Prevention tools typically do not take user behavior into account at all, and traditional User Behavior Analytics solutions rely on log files for visibility – which leave out an important portion of the story. Without endpoint visibility, it's difficult both to stop infiltrators early and to reverse-engineer a forensic timeline after an attack.

Security teams can **catch these signs early only as long as they are able to identify unusual user behavior.** If John the Accountant suddenly starts escalating

his own account privileges and looking at sensitive engineering documents, that's an immediate sign that something clearly suspicious is happening. **By acting quickly, you can stop the attack before the worst of it occurs.**

What's more, infiltration or credential theft is **rarely a one-hit attack.** We typically see that hackers will infiltrate an organization or steal credentials, and then sell that access on the dark web – **meaning that your organization could get hit again, and worse, weeks or months down the line.** This is why full remediation and frequent credential updates are critical.

REAL WORLD SPOTLIGHT: THE DNC HACK

The world saw the ramifications of infiltration illustrated all-too-vividly this past year in a particularl high-profile case: the hack of the Democratic National Committee. The DNC hack was the result of an insider falling prey to a phishing attack and clicking on a bad link, even though the Clinton campaign itself regularly tested staffers with phishing tests. If the DNC had been better prepared to monitor for insider attacks, and had the means to mitigate them, the breach may not have escalated into the massive event that it did.

PART FOUR

THE SOLUTION

Tackling insider threat prevention can be intimidating. The category is so broad that it's impossible to narrow down remediation to one simple solution, and it's especially difficult to pinpoint dangerous acts from inside your organization. An insider threat prevention program needs to take a flexible, intelligence-based approach in order to be successful – and oftentimes, it forces security teams to look outside the box.

1. LOOK BEYOND BLOCKING
2. SET CLEAR GUIDELINES AND EDUCATE EMPLOYEES
3. VISIBILITY IS KEY
4. BUILD ON INTELLIGENCE

How do you fight insider threats?

DETECTION AND PREVENTION

At Dtex, we have spent years studying insider threats. Preventing user threats will never be easy or straightforward, and there is no single bulletproof solution. Despite spending millions of traditional security measures, enterprises still have blind spots in their protection, and they still fall victim to breaches and data theft. To build upon these tools and close the gaps, there are several things security teams can do to significantly mitigate their risk:

LOOK BEYOND BLOCKING

Many enterprises rely on Endpoint DLP and similar tools to stop employees from using certain tools, going to certain websites, or copying certain files. While blocking tools have their place as one part of a security ecosystem, modern enterprises can no longer rely on them as their *only* form of endpoint security for two main reasons:

1. **The technological world is evolving too rapidly.** It is impossible to block every single potential method of data exfiltration. New file sharing sites, cloud hosts, transfer methods, and other technologies are popping up each and every day. Since Endpoint DLP solutions rely on specific rules, your security team cannot possibly keep up with the rate of advancement.
2. **Distributed enterprises need modern tools** – even if they could potentially threaten security. To our previous point, even if you could block every single file sharing website, for example, would you want to? In a modern world where companies span states, counties, and continents, employee productivity is contingent upon

REAL WORLD SPOTLIGHT: CLOSING THE GAP

Dtex customers frequently use Dtex to fill in gaps in Endpoint DLP. For example, a large technology company used Endpoint DLP to alert on possible data theft, but could not contextualize those alerts. DLP could tell them when files were leaving the organization through personal email or other risky file transfer methods, but if the data was in an encrypted file, DLP had no visibility. As a result, this customer set up rules to alert every time an encrypted file was sent via personal email — then, an analyst would have to manually triage this alert by decrypting the files or accessing the end user's machine. As one might imagine, this was a major blind spot, as well as inefficient. Dtex gave this customer the visibility to easily see which files were going into encrypted archives, closing the gap.

having the flexibility to quickly and easily communicate, share, and produce. Blocking every potential threat would create a workplace that was, at best, slow and frustrating – and at worst, hostile.

While blocking can be *part* of the solution, **it isn't the only solution**. DLP needs to be supplemented with a flexible, visibility-based solution that allow security teams to see what it's missing and adjust accordingly. The right solution will complement DLP and other traditional security layers to catch the threats that are slipping through the cracks.

SET CLEAR GUIDELINES AND EDUCATE EMPLOYEES

Far more than half of the security incidents Dtex Assessments have uncovered were accidental, not malicious. While no company will ever be able to totally eliminate accidental security risks, **education is a critical part of prevention.** Lay out clear guidelines for how employees should use technology, and teach them how to recognize suspicious emails and programs by running phishing and social engineering tests. When you do catch potentially dangerous negligent behavior, **use it as an educational moment and make sure that the user in question knows what they did wrong and how to avoid it next time.**

VISIBILITY IS KEY

In order to know what users are doing both on and off your corporate network, security teams need to have visibility from the point closest to the user: **the endpoint.** Visibility into user behavior is not a replacement for traditional security tools, but it is a critical supplement. Network based visibility has huge gaps, since so many methods of data exfiltration can happen completely offline or, even more commonly, off the corporate network. Detecting and remedying insider threats begins with having true visibility into user behavior. A strong visibility program complements a full security program and strengthens the immune system of the enterprise.

BUILD ON INTELLIGENCE

The next step is to build upon that user visibility with behavior intelligence. This means investing in an analytically-based solution that can **tell your security team when behavior dramatically changes from the norm** – this is the best way to tell if a user is stealing data, or if their account has been infiltrated by a third party. These solutions are also a more flexible way to see when users are handling data in a risky manner, even if they are doing so unintentionally.

What is hiding in your enterprise?

GET YOUR RISK 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 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. In 2015, Dtex secured $15 million in Series A funding led by Norwest Venture Partners and Wing Ventures. To learn more, visit www.dtexsystems.com.