What's the biggest detriment to your organization's data?

It's not what you think.

Everybody knows about the threat that hackers present to your data. But it's your employees that present the bigger risk by unknowingly granting hackers access to your organization. In Intermedia's 2017 Data Vulnerability Report, we surveyed 1,000+ full-time office workers at companies of all sizes to find out how workplace behaviors are impacting data security.

While 70% of employees say that their company provides regular cyber security risk training, the reality is office workers are lax at adhering to security best practices. Education efforts don't extend far enough. The number of phishing scams is higher than ever, and office workers aren't being properly trained to circumvent this exponential risk. As a result, a false sense of employee confidence is having financial ramifications on organizations of all sizes.

We'll be releasing findings as part of an ongoing three-part series, looking at the impact and outcome these habits have regarding email breaches and threats, ransomware, and data loss, and what you should do about it.

SHARE THIS REPORT

Email Breaches and Threats

Vulnerability and Victims

PHISHING, THE PROCESS BY WHICH CYBER CRIMINALS ATTEMPT TO COERCE EMAIL VICTIMS INTO MAKING A FINANCIAL TRANSACTION, DISCLOSING LOGIN CREDENTIALS OR VISITING A MALWARE-LADEN WEBSITE, IS ONLY GETTING WORSE

ACCORDING TO THE FBI, BUSINESS-EMAIL COMPROMISE SCAMS ACCOUNTED FOR MORE THAN $5 BILLION IN LOSSES BETWEEN OCTOBER 2013 AND DECEMBER 2016

Research reveals a false sense of confidence among office workers with phishing scams still on the rise

14%

One in seven survey respondents are not confident in their ability to detect a phishing email or they do not know what phishing is

21%

Roughly one in five office workers have been a victim of a phishing email

EXPRESS BEING CONFIDENT IN THEIR ABILITY TO DETECT A PHISHING EMAIL

OF OFFICE WORKERS HAVE BEEN VICTIMS OF A PHISHING EMAIL

Phishing, It's Not Just for Entry-Level Employees

REPORT THEY HAVE BEEN THE VICTIM OF A PHISHING EMAIL, MORE THAN OTHER GROUPS OF KNOWLEDGE WORKERS

Ryan Barrett,
VP of Security and Privacy, Intermedia

It's no longer effective to just talk 'at' employees about cyber threats. Companies need to offer regular interactive IT security training events to show employees what real attacks look like, and how to react to them. For example, at Intermedia we do a Hacktober event every October where we simulate 'live' security incidents to help employees detect and prevent cyber-attacks in a fun and interactive way.

While the number of attacks has dramatically increased in the past two years, employee training has not

ORGANIZATIONS REGULARLY COMMUNICATE OR TRAIN EMPLOYEES ABOUT CYBER THREATS AS A MEANS OF PREVENTION

What companies deem to be "regular" communication

ACCORDING TO INTERMEDIA'S 2016 IT CONFIDENCE INDEX SURVEYED IT PROFESSIONALS SAID

their company offers no such training at all

their company offers interactive IT security training to their employees quarterly

their company offers interactive IT security training at least once every six months

WHY ARE EMPLOYEES STILL TAKING THESE RISKS AND WHAT SHOULD COMPANIES BE DOING TO PREVENT IT?

Ryan Barrett,
VP of Security and Privacy, Intermedia

When it comes to devising trainings, companies need to think outside of the box. How do you track effectiveness? For example, we've even simulated a phishing attack among our own employees because we've found that the percentage of employees that fall victim to these self-imposed exercises goes down dramatically with each internal attempt. Interactive phishing campaigns allow employers to safely educate employees without risking the loss of valuable data.

HOW CAN CHANNEL PARTNERS HELP THEIR CUSTOMERS CIRCUMVENT THESE RISKS?

Eric Martorano,
Chief Revenue Officer, Intermedia

Offering frequent interactive trainings might be achievable for larger companies, but it can be challenging for smaller organizations. SMBs are frequently limited by technical and/or financial resources to protect their data effectively, making them a prime target for cyberattacks. For MSPs, providing comprehensive security training in tandem with layered security solutions presents a prime opportunity to deliver additional value in a much-needed area.

As ransomware attacks grow in sophistication, both employees and employers are paying ransoms in record numbers

Part 2 of Intermedia's 2017 Data Vulnerability Report examines the critical security behavioral habits of more than 1,000 office workers related to ransomware.

Our findings revealed that while companies do provide regular cyber security training, office workers continue to be lax on adhering to security best practices which can cause significant financial ramifications to organizations of all sizes.

Despite headlines around WannaCry, Petya, and other ransomware outbreaks, as well as efforts around employee education, confusion in the workplace remains regarding what ransomware is and how it gets delivered. Subsequently, both employers and employees are paying ransoms at record rates...when they don't need to.

SHARE THIS REPORT

Ransomware attacks continue to grow exponentially

The threat of ransomware, when hackers infect devices with a virus and hold data hostage until a sum of money has been paid, is only getting worse.

ACCORDING TO THE FBI, GLOBAL RANSOMWARE DAMAGE COSTS ARE PREDICTED TO EXCEED $5 BILLION IN 2017, WHICH IS UP FROM $325 MILLION IN 2015, AS REPORTED BY THE CYBER THREAT ALLIANCE

SECOND ONLY TO HARDWARE FAILURE (50%), OFFICE WORKERS SAID RANSOMWARE/ CYBERATTACKS (29%) WERE THE BIGGEST THREAT TO DATA LOSS WITHIN THEIR ORGANIZATION

Even with the increased publicity and impact of global ransomware attacks, awareness still lags:

In 2016, **89%** of IT professionals were at least moderately confident that employees in their company would be able to identify an attempted ransomware attack

However, **31%** of office workers admit they aren't familiar with ransomware

MEN REPORT GREATER LEVELS OF AWARENESS THAN WOMEN

78% of **male** office workers say they know what ransomware is

60% of **female** office workers say they know what ransomware is

It's not for lack of effort though...

70% of office workers said their organization regularly communicates about cyber threats

THIS INCLUDES COMMUNICATING WITH EMPLOYEES ABOUT LARGE-SCALE GLOBAL RANSOMWARE ATTACKS...

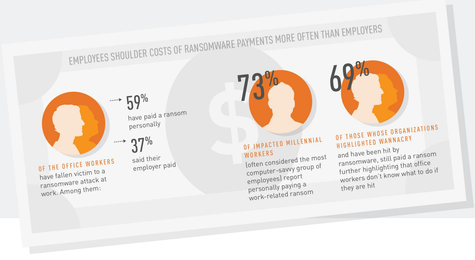
30% said their organization specifically highlighted the **WannaCry ransomware attack** as an example

Jonathan Levine,
CTO, Intermedia

As ransomware continues to evolve and become more advanced, organizations of all sizes and types must acknowledge it as a very real threat. This is especially true for SMBs that may not have the resources, tools, or training that larger organizations use to recognize, prevent and protect themselves from such attacks. Ransomware can infiltrate and shut down an entire business through one infected computer. More often than not, SMBs feel they are forced to pay a ransom they can't, but must, afford. And hackers realize this.

The hidden costs of ransomware

WHILE THE MAJORITY OF COMPANIES COMMUNICATE ABOUT THE THREAT RANSOMWARE PRESENTS, EMPLOYEES AREN'T ALWAYS TOLD WHAT TO DO IF THEY ARE A VICTIM. IN FACT, DATA SHOWS THAT OFFICE WORKERS TAKE ACTIONS THAT COULD DRAMATICALLY UNDERMINE SECURITY EFFORTS.



THERE ARE A NUMBER OF REASONS WHY EMPLOYEES WOULD PAY THE RANSOM THEMSELVES

Employees may see paying the ransom out of their own pockets as the quickest and easiest way to get their data back, when in actuality, 15% of the time the data isn't released, even after the ransom is paid. Organizations need to focus education efforts not just on what ransomware is, but what steps employees should take if they are impacted.

How can you protect your organization? – an Intermedia customer weighs in

WITH PROPER PLANNING, YOU CAN AVOID PAYING THE RANSOM

Two years ago, we were hit by a very good social engineering ransomware attack. A cyber criminal emailed the exploit to a hiring manager as an attachment labeled, 'resume.zip' referencing an open position we had. It was 4pm on a Friday, and so by the time the individual had realized what had happened Monday morning, around 100,000 files were encrypted. Because we had taken proper business continuity planning measures, we were able to do a mass rollback of the infected files. We didn't pay any ransom and suffered no data loss. We've also changed our policy to add Zip files to the list of executable files that are blocked by our email filter.

Joshua Sharfman,
Chief Technology and Innovation Officer, California Association of REALTORS

CREATING A MORE AWARE COMPANY CULTURE

Twice a month, we provide cybersecurity education. We also conduct company contests. For instance, after the Equifax breach, we held email contests to identify four potential risk areas within a dummy email. Following the hurricanes, we notified employees that after disasters, there are often exploits trying to get people to donate to seemingly legitimate causes. The sad reality is companies need to assume that they are vulnerable. It is not a matter of if, it is a matter of when. In addition to having an incident response plan ready to go, talk to employees regularly. Humans are generally the weakest link. We're all best served by helping everyone to maintain a high degree of awareness. Create a company culture where employees know to seek assistance if they are suspicious, ideally before, but also after they click.

Ransomware and the channel – an Intermedia partner weighs in

HOW INTERMEDIA'S SECURITY SUITE HELPS PARTNERS TO DIFFERENTIATE

Koert Council,
Partner at Kosh Solutions

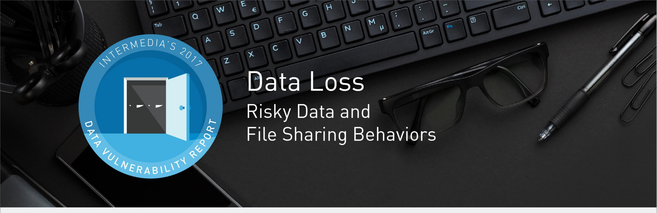
The prevalence of high-impact cyberattacks has changed the way that organizations need to approach security. This presents MSPs with a security specialization the opportunity to help clients better prepare and safeguard against these threats, while scaling their own business. For instance, the surge in ransomware attacks is a significant driver of our new customer signups. Intermedia's backup and file sharing solution enables us to restore clients' access to impacted documents in just minutes following a range of scenarios, from stolen or damaged devices to ransomware attacks and other mass infections. Intermedia's security services suite gives us a huge market differentiator.

Now what should you do?

Integrate ransomware education into your broader data breach and cybersecurity training efforts. However, it's not enough to just identify the risk. These regular communications must explain what employees should do if they are hit. Otherwise, as our report identifies, employees could take matters into their own hands. It's these actions that could undermine security efforts, and result in days (if not weeks) of downtime. Be sure to have a solid business continuity plan in place to keep your business up and running in the event of a ransomware outbreak, including installing a continuous backup product such as Intermedia's SecuriSync®.

Ideally, if you have proper backup in place, you won't have to worry about paying a ransom in the first place. Don't worry if this sounds like a lot to take on yourself. Intermedia can help you develop an ongoing plan, in addition to identifying local resources that can assist with implementation process.

Check out the resources below for further information on preventing ransomware attacks, and to sign up to receive the 3rd installment of our report on risky data and filing sharing behaviors.



Data Loss

Risky Data and File Sharing Behaviors

99% of Office Workers Commit Actions that Dramatically Increase the Likelihood of a Workplace Data Breach

In the third and final part of our 2017 Data Vulnerability Report, we analyze the impact and outcome of 1,000+ full-time office workers' habits relative to data loss, how it's happening, and what can be done to mitigate the risk.

Office workers often ignore data security best practices, putting themselves and their employers at great risk

THAT UNDERMINES WORK EMAIL AND DOCUMENT SECURITY

The threat of ransomware, when hackers infect devices with a virus and hold data hostage until a sum of money has been paid, is only getting worse.

Almost all (99%) of the professionals surveyed admitted to conducting at least one potentially dangerous action, from sharing and storing login credentials to sending work documents to personal email accounts.

When it comes to storing and sharing data and saving login credentials, employees prioritize personal convenience over security protocols. By ignoring data security best practices, office workers are putting themselves and their employers at great risk. In fact, it's often the employees that pose the biggest risk to data loss, including those in IT departments who you'd think would be more aware and vigilant.

Lost or stolen data can significantly impair an organization, and the impact is only getting worse as the frequency and sophistication of cyberattacks increase.

24,000

IN 2017, THE AVERAGE SIZE OF DATA BREACHES GREW TO INCLUDE MORE THAN 24,000 RECORDS

While employees may worry, convenience is still king

Despite nearly one quarter (23%) of employees worrying that someone outside of their company could hack or access files due to an email breach, they continue to ignore best practices opting instead for more convenient, and therefore more detrimental, practices.

Jonathan Levine,
CTO, Intermedia

While widespread ransomware attacks, hardware failure, and natural disasters are all serious threats to an organization, sometimes the biggest security threat comes from the inside. When employees do not properly back up files, choose to use the same password across multiple accounts, or send confidential materials to their personal accounts, their companies are left exposed and vulnerable not only to data loss, but to serious financial and legal implications as well.

WHEN IT COMES TO STORING/SHARING DATA, AND SAVING LOGIN CREDENTIALS:

ROUGHLY 1 in 4
(24%) of office workers **reuse the same login credentials** for their work and personal accounts

NEARLY All
(96%) of office workers **automatically save work passwords on their work computer**, instead of routinely entering login credentials

ROUGHLY 2 in 4
(42%) of office workers surveyed in Intermedia's 2015 Insider Risk Report said that they had **used their personal password for business applications**

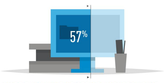
ALMOST 1 in 4
(23%) of office workers **admit they automatically save their work credentials** to their home computer

35% OF MILLENIALS

19% OF GEN X

12% OF BOOMERS

use the same login credentials for work and personal accounts



MORE THAN HALF OF OFFICE WORKERS ADMIT TO STORING WORK FILES ON THEIR DESKTOP OR IN DESKTOP FOLDERS

1/3 SAY THEY STORE WORK DATA ON PERSONAL FILE SYNC AND SHARE SERVICES, A SIGNIFICANT INCREASE FROM THE 12% WHO REPORTED DOING THIS IN 2015

While employees may find these practices to be more convenient, they leave their organizations and networks more susceptible to cyberattacks. Considering that market researcher Cybersecurity Ventures predicts worldwide cybercrime damages will increase to $6 trillion annually by 2021, with risky employee behaviors helping to fuel that rise, it's clear that there is a great deal of education, as well as sweeping changes to habits, policies, and procedures, that must take place.

Jonathan Levine,
CTO, Intermedia

Employees want to do the right thing, but sometimes don't know how, or the tools they are given to do so are often hard or cumbersome to use. As our latest study shows, organizations need to recognize that getting employees to change their behavior won't happen overnight. Instead, companies need to offer solutions that protect confidential information with minimal impact on an employee's daily workflow, such as automated backup and 2-factor password requirements. The most effective security measures are often ones that employees don't even know are in place.

Employees increasingly share confidential company documents via insecure ways

Just as, if not more, worrisome is the amount of proprietary data and intellectual property that employees are passing back and forth between their work and personal accounts.

While this is most common when an employee leaves a company, current employees also engage in this behavior, increasingly putting companies at risk and vulnerable to data loss.

ACCESSING MATERIALS AFTER LEAVING A COMPANY IS ON THE RISE, ESPECIALLY IN I.T.

EMPLOYEES PASS SECURE DATA BACK AND FORTH AT LEAST ONCE A WEEK USING UNSAFE METHODS:

of office workers email a work document to their personal email at least weekly, exposing confidential data to even more threats

...and they aren't just sharing emails or memos. THESE MATERIALS INCLUDE:

22% HR-RELATED INFORMATION **19%** CUSTOMER INFORMATION **18%** THE COMPANY'S STRATEGIC INFORMATION

How can you mitigate the risk your employees pose?

Joshua Sharfman,
Intermedia customer and Chief Technology and Innovation Officer at California Association of REALTORS

The research indicates that the most vulnerable security breach vector within an organization is your employees. For example, they get lazy with passwords and reuse credentials. They're not mindful of emails and aren't vigilant when clicking on embedded links.

Having appropriate system policies in place is also key, and Intermedia's technology helps us do that. I also recommend that companies block the payloads that they don't want coming into the network because they could carry executable malware and create other ways of transporting that data. Also, it's important to apply proper patches and updates in a timely manner. Data security is all part of the operational expense, and a critical one that is frequently overlooked.

Beyond educating employees on potential risks that lead to data breaches, choose security solutions that protect confidential information with minimal impact on daily workflow. This includes real-time automated backup that enables quick file recovery, if needed, but doesn't require any action of employees. Not sure what to do next? Don't worry. Intermedia can help you identify a solution that's right for your business.