Dell End-User Security Survey 2017

TABLE OF CONTENTS

INTRODUCTION

When the unauthorized sharing of confidential data makes headlines, it's typically attached to a scandal – like when WikiLeaks has published reports from anonymous whistle blowers or a company has sued their competitor for using trade secrets pilfered by a former employee. However, confidential data sharing happens under more mundane circumstances every day in businesses around the world.

In most cases, there are no repercussions for the employees sharing this data, as organizations' security teams may not even be aware of the protocol breach and nothing untoward happens. This lack of immediate action makes it all too easy for employees to dismiss the risks and continue breaking security protocol. But eventually, a file ends up in the wrong hands and the company finds itself at the center of a devastating situation that can be disastrous either financially or for the company's corporate reputation.

To find out how widespread the unsafe sharing of confidential data has become, Dell commissioned a global survey of 2,608 professionals who handle confidential data at companies with 250 or more employees. The results show a staggering 72 percent of employees are willing to share sensitive, confidential or regulated company information.

72%

of employees are willing to share sensitive, confidential or regulated company information

In most cases, their motives are not malicious – they are simply trying to do their jobs as efficiently and effectively as possible. There are a multitude of legitimate business reasons for sharing confidential information. However, the survey results you will read in this report make it clear that many companies are still lacking the policies and procedures to ensure this data sharing is done in a secure manner. The findings also reveal that even employees who have been educated on the risks of sharing confidential data without following security protocols have not fully "bought into" the consequences that can arise from this behavior. They understand their actions are risky yet still are not deterred by the potential consequences, which feel ethereal compared to the tangibility of their daily workplace tasks.

The Dell End-User Security Survey paints a picture of a workforce caught between two imperatives: be productive and efficient on the job, and maintain the security of company data. To ease the friction between these competing goals, companies must focus on educating employees as well as enforcing policies and procedures that secure data wherever they go, without hindering productivity.

We hope these findings are illuminating for both security and IT professionals, as well as business managers tasked with safeguarding data and ensuring productivity for the organization.

Employees Likely to Share Confidential Information

From an employee's perspective, there is a great deal of gray area surrounding what entails authorized sharing of data. Most employees may recognize they shouldn't email a customer's credit card information to anyone under any circumstance. But is it acceptable to share a confidential product roadmap with a vendor if an employee's manager tells him or her to do so? What about sharing a brief on an unreleased product with the marketing team's copywriter so he or she can prepare web copy? As the Dell End-User Security Survey reveals, there are a number of circumstances under which it makes sense to share confidential information in order to push business initiatives forward.

Nearly three in four (72 percent) employees say they would share sensitive, confidential or regulated company information under certain circumstances. The most cited circumstances include: being directed to do so by management (43 percent); sharing with a person specifically authorized to receive it (37 percent); determining that the risk to their company is very low and the potential benefit high (23 percent); feeling it will help them do their job more effectively (22 percent); and feeling it will help the recipient do their job more effectively (13 percent).

72%

of employees say they would share sensitive, confidential or regulated company information under certain circumstances

directed to do so by management

sharing with a person authorized to receive it

the risk is very low and the benefit high

it will help them do their job more effectivelv

it will help the recipient do their job more effectively

However, in many of these circumstances, the employee making the judgment call on whether or not to share the confidential data is operating independently. This leaves the employee responsible for properly gauging the risk or benefit of sharing certain types of information.

That's one of the reasons why it's common for cyber thieves to pose as a trusted partner, employee or organization to convince employees to share sensitive data. More than one in three employees (36 percent) will frequently open emails from unknown senders at work, potentially opening the door for spear phishing attacks in which a cybercriminal seeks unauthorized access to sensitive information from a specific organization or individual by posing as a trusted source. When security becomes a case-by-case judgement call being made by hundreds or even thousands of employees, it loses its consistency and efficacy.

Certain industries deal with corporate information that is more easily categorized as highly sensitive, but still employees may be willing to share sensitive data under certain circumstances. Nearly four in five employees in financial services (81 percent) will share sensitive, confidential or regulated company information. This means that among the top four banks in the United States, more than 586,000 employees have the propensity to share sensitive data.[i] Employees in education (75 percent), healthcare (68 percent) and federal government (68 percent), while still less likely to share data than financial services employees, also share confidential or regulated data on occasion.

To protect sensitive corporate information, a company's primary role is to define the circumstances under which information can be shared and with whom, covering as many scenarios as possible to give employees the guidance they need to make wise day-to-day security decisions. However, it's also important to note that when data sharing happens, it must be done securely.

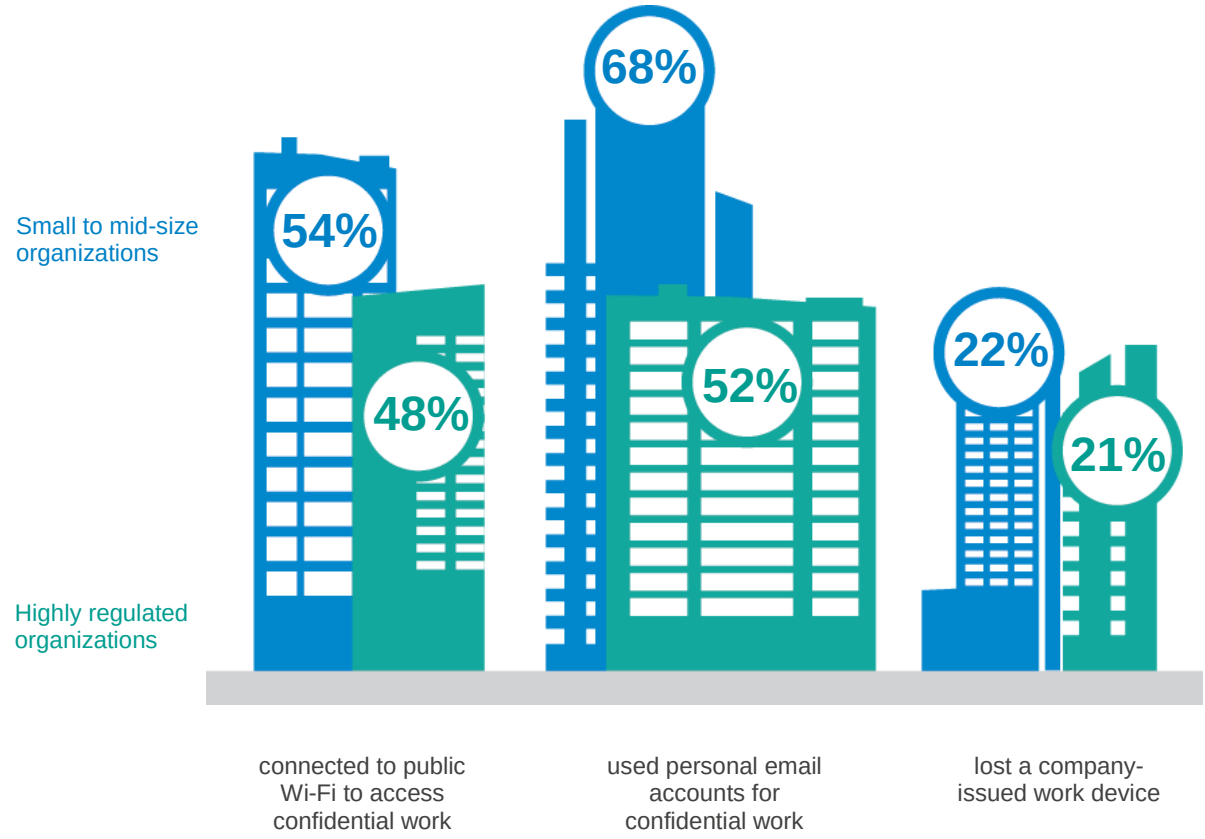
The next set of survey findings shows that the real danger may lie not in what information is shared, but in how it's done.

Unsafe Behaviors Common in the Workplace

Employees' willingness to share sensitive data is not the primary issue uncovered in the Dell End-User Security Survey. What is much more troubling is that when employees do share or interact with confidential data, they often do so insecurely.

Forty-five percent of employees across organizations admit to engaging in unsafe behaviors throughout the workday. These behaviors include connecting to public Wi-Fi to access confidential information (46 percent), using personal email accounts for work (49 percent), or losing a company-issued device (17 percent).Those in highly regulated organizations engage in unsafe behaviors at even higher rates: 48 percent say they have connected to public Wi-Fi to access confidential work information, more than half (52 percent) have used personal email accounts for confidential work communications, and more than one in five (21 percent) have lost a company-issued work device. These numbers are even higher among employees of small to mid-size organizations.

45% of employees across organizations admit to engaging in unsafe behaviors throughout the workday



Perhaps one of the most shocking findings is that more than one in three employees (35 percent) say it's common to take corporate information with them when leaving a company. This situation has recently proven problematic for Facebook and Uber, who have been sued on the grounds that executives at their subsidiary companies (Oculus Rift and Otto, respectively) stole trade secrets when the left the plaintiffs' employer.[ii] [iii]

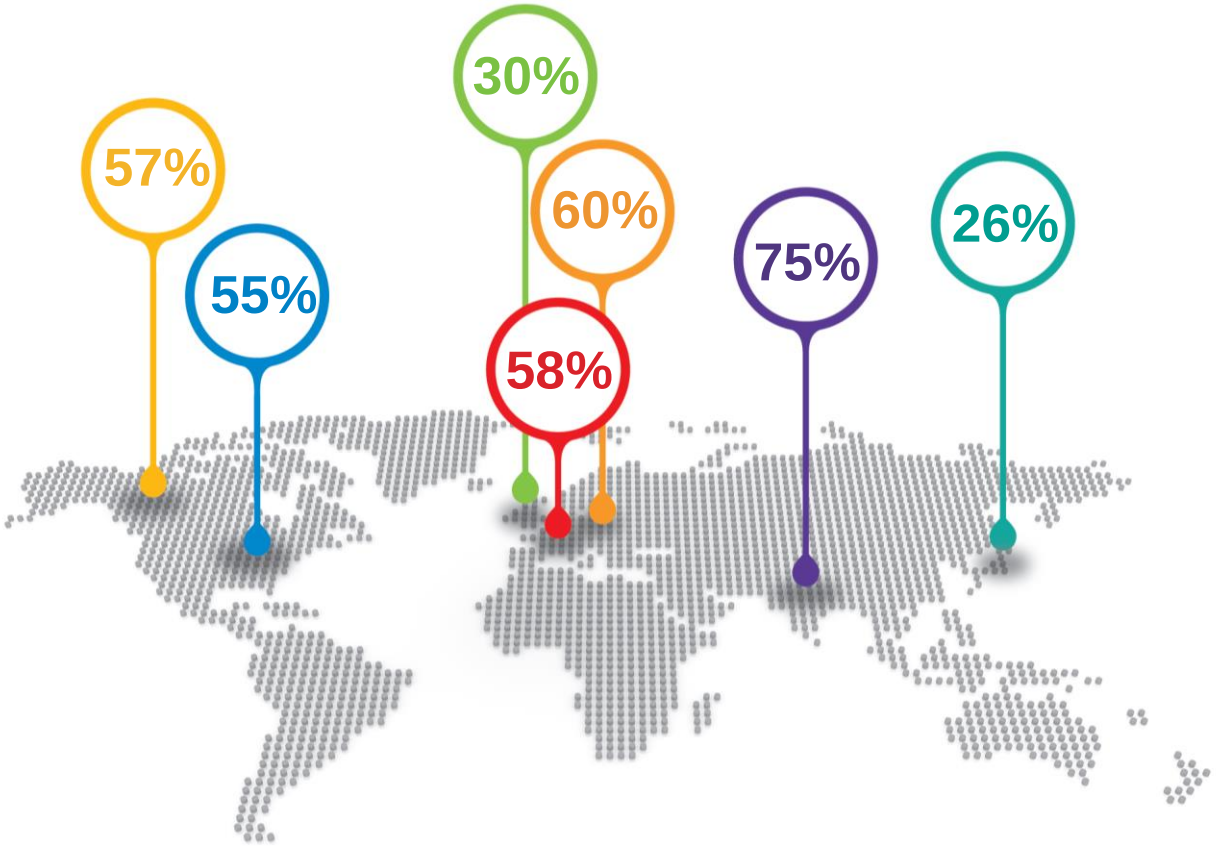
The survey found that there are cultural differences that may influence whether employees leaving a company take data with them. It's most common for employees in India (57 percent) to take corporate information with them and least common for employees in Japan (15 percent). Most employees who take information take samples of work they have personally completed (36 percent), but 16 percent will take work that others have completed. Typically, employees either transport the company data on a USB drive (61 percent) or via email (56 percent), both of which are difficult methods for organizations to track or block.

Interestingly, three percent of the employees across organizations admitting to engaging in unsafe behaviors say they did so with malicious intent. However, 24 percent say they just wanted to get their job done, and 18 percent say they didn't know they were doing something unsafe. Each of these scenarios represents a vastly different problem for companies to address, showing security gaps ranging from insider threats to a lack of effective security education.

This lack of education may cause even more widespread problems for companies with BYOD programs. Of employees who use a personally-owned device to access confidential work information, 62 percent are personally responsible for managing the device's security, while only 28 percent of organizations assign that responsibility to their IT team. If employees are unsure what constitutes risky behavior, their ability to effectively secure their own devices is probably limited.

It's this same overarching lack of security knowledge that has led to the popularity of social engineering as a cyberattack method, in which a cybercriminal tricks individuals into breaking security procedures or disclosing sensitive information. Cybercriminals have realized it's easier to convince victims to provide their passwords than it is to guess them. All the criminal has to do is gain the trust or interest of their marks, for example by creating a quirky, fun survey designed to bait visitors to give out sensitive information like the street you grew up on, the name of your first pet or your mother's maiden name. This is particularly concerning for businesses because nearly half of employees (49 percent) use corporate-issued devices to access their personal social media accounts, sometimes more depending on the culture. In India, three in four employees access personal social media accounts from their work devices, while employees in the U.S. (55 percent), Canada (57 percent), France (58 percent) and Germany (60 percent) also exceed the global average. On the other hand, only 30 percent of employees in the U.K. and 26 percent in Japan use their work devices to access personal social media accounts.

49% of employees use corporate-issued devices to access personal social media accounts



Employees may also be taking on unnecessary risks in how they store and share their work. Fifty-six percent of employees use public cloud services such as Dropbox, Google Drive, iCloud and others for sharing or backing up their work, with 53 percent using a personal account—versus a corporate account—to access cloud services.

When it comes to sharing confidential files with third-party vendors or consultants, 45 percent of employees use email. However, nearly one-third (31 percent) say third-party vendors or consultants have access to their company's intranet or other internal information system, which may be even riskier if those vendors' access is not limited correctly. Target famously experienced a breach in 2014 when a cyber attacker accessed the retailer's network using the credentials assigned to their third-party HVAC vendor.[iv]

As the workforce become more flexible – in terms of the devices they use, the places they store data, and the locations they work from – the risk of lost or stolen sensitive data grows immensely. Companies should not only focus on standardizing the process of when data should be shared and with whom, but also how that data gets shared and what happens to it once an employee leaves the company.

Employees Support Protecting Information, but Don't Feel Empowered

As the Dell End-User Security Survey reveals, employees tend to have a love-hate relationship with cybersecurity in the workplace. While they do not want to see their company suffer a data breach and even feel responsible for helping keep information secure, they struggle with the limitations security programs can put on their day-to-day activities.

Nearly two in three employees (65 percent) feel it is their responsibility to protect confidential data, including educating themselves on possible risks and behaving in a way that protects their company. However, only 36 percent of employees feel very confident in their knowledge of how to protect sensitive company information.

Although the majority of employees feel it is their responsibility to protect company information, they face a number of hurdles in doing so. Twenty-one percent say the security put in place by IT slows down their work, while 21 percent feel it's difficult to keep up with changing security guidelines and policies. Employees even express concern with their inability to effectively protect corporate data, with 22 percent saying they are worried that someday they will do something by mistake and cause real damage for the company.

While facing personal challenges in protecting confidential data, more than three in four employees (76 percent) also feel their company prioritizes security at the expense of employee productivity. Still, even while feeling hampered by security, employees say they don't know how to keep sensitive information secure.

Education may seem like a clear solution for this lack of security knowledge and confidence. Yet although nearly two in three employees (63 percent) are required to complete cybersecurity training on protecting sensitive data, 18 percent of employees still conducted unsafe behavior in the workplace without realizing what they were doing was wrong. Moreover, 24 percent of cybersecurity-trained employees conducted unsafe behavior because they just wanted to get their job done.

There is no one-size-fits-all solution to this issue, because every company has different security needs. However, it's clear that corporations and employees must meet somewhere in the middle. Though many employees already complete cybersecurity training, management may also need "training" from employees to fully understand their daily tasks and scenarios in which they might feel justified in sharing confidential data.

FINAL TAKEAWAYS

Of all the findings uncovered by this survey, it is perhaps most disheartening that nearly two out of three employees who handle confidential data are being trained on cybersecurity, but still don't know how to keep sensitive information secure. Even when they are aware of the best practices, they are willing to overlook them when necessary to get their job done.

This points to a key issue: company policies on confidential data usage and sharing are either unclear or not comprehensive enough to cover the spectrum of daily scenarios employees encounter in the workplace. Organizations must stop simply telling employees not to share confidential information and instead unlock the ability for them to share confidential data when it makes sense, but in a secure and simple fashion.

The only way to solve these challenges is for organizations to strive for higher levels of awareness, enablement and protection simultaneously:

- Create simple, clear policies and ensure they outline steps for handling common scenarios that employees experience. Policies are key for preventing breaches and data loss, but first businesses need to identify what is important to them – both endpoint devices and critical data – and write down policies that define end-user access, types of data, who can have access to the data and rules for its dissemination outside of the organization. The goal is that at least 99 percent of workers understand why security is important and do their best to comply throughout their day, no matter the device they're working on, the location they're working from or the people they're working with.

- Embrace and enable productivity. The most secure environment is one that's disconnected from the internet, but of course that's not realistic. What's needed is the confluence between security and productivity. If data security policies encumber workforce momentum, employees will find a way around them. Security should not limit business initiatives, but support them through closer alignment between an organization's C-Suite and IT teams. This perfect balance can be different for each company, but a balance must be reached.

- Use security solutions that protect data wherever they go. Organizations need to safeguard data not only as they reside on PCs and mobile devices, but also as they are shared in the cloud, sent to a personal email account or transferred to an external device. Keeping data safe requires a comprehensive solution – one that can protect, control and monitor the data wherever they go. Organizations need to be able to control who gets access to the data, monitor where the data are and how they are used, and be able to apply rights and polices so that only the right people can access them under the right circumstances. Deploying a robust, multi-layer security infrastructure that protects data without interfering with workflows and employee productivity will safeguard organizations from data loss.

The Dell End-User Security Survey shows that organizations have to accept two truths: confidential data will be sent, stored and accessed on a daily basis, and employee training alone is not going to keep corporate information secure. It's imperative that organizations design their security program to implement a combination of solutions that address security awareness, enablement and protection among the workforce. If companies are going to keep their data truly safe amid an ever-evolving threat landscape, they need clear protocols in place that are backed by a realistic understanding of employees' day-to-day responsibilities, as well as technology that protects sensitive data wherever they go – whether at rest, in motion or in use.

METHODOLOGY

Dimensional Research conducted an online survey commissioned by Dell Data Security among 2,608 professionals that personally have access to and work with confidential, sensitive or regulated data and information at companies with more than 250 employees. Participants were surveyed across eight countries, including Australia, Canada, France, Germany, India, Japan, the United Kingdom and the United States. The research was conducted from February 24 to March 9, 2017.

ABOUT DIMENSIONAL RESEARCH

Dimensional Research provides practical marketing research to help technology companies make smarter business decisions. Our researchers are experts in technology and understand how corporate IT organizations operate. Our research services deliver a clear understanding of customer and market dynamics. For more information, visit www.dimensionalresearch.com.

ABOUT DELL INC.

With award-winning desktops, laptops, 2-in-1s and thin clients, powerful workstations and rugged devices made for specialized environments, monitors, endpoint security solutions and services, Dell gives today's workforce what they need to securely connect, produce, and collaborate from anywhere at any time. Dell, a part of Dell Inc., services customers from consumers to organizations of all sizes with the industry's broadest, most innovative end-user portfolio.

---

[i] "Leading banks in the United States as of December 31, 2016, by number of employees," Statista, https://www.statista.com/statistics/250220/ranking-of-united-states-banks-by-number-of-employees-in-2012/

[ii] Selena Larson, "Facebook loses $500 million Oculus lawsuit," CNN Money, February 2, 2017, http://money.cnn.com/2017/02/01/technology/zenimax-oculus-lawsuit-500-million/

[iii] Reuters, "Uber to Push for Arbitration in Waymo Trade Secrets Theft Case," Fortune, March 16, 2017, http://fortune.com/2017/03/16/uber-arbitration-waymo/

[iv] "Target Hackers Broke in Via HVAC Company," Krebson Security, Feb. 5, 2014, https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/