DELL Technologies

Workplace Security Report 2019

Introduction

Corporate data breaches are on the rise as hackers evolve their tactics to compromise systems, endpoints and individuals to steal valuable information. Organizations are deploying more user devices, public cloud infrastructure and connected Internet of Things devices in an effort to transform with the digital economy, resulting in more vulnerability points than ever.

A cybersecurity attack can not only tarnish a company's reputation and break the trust of employees, customers, and shareholders, but the subsequent downtime to contain and remediate the issue can result in both significant financial and productivity losses and affect future business.

From March 2018 to March 2019, Dell Technologies conducted several independent studies, covering more than 4,600 global executives and managers, 2,200 global IT decision makers, 12,086 global high school and college students, and 1,050 full-time employed adults in the U.S. The purpose of these studies was to understand the state of corporate data protection and digital transformation strategies, as well as how the current and future workforce views security from the ground up.

The **Dell Technologies Workplace Security Report** examines the trends and insights revealed across these studies, highlighting the security challenges facing organizations and the workforce today. We believe you'll find this information helpful as you embark on or continue your digital transformation journey, from security and IT professionals tasked with safeguarding data to managers and business leaders responsible for employee development and company growth.

Key Findings

Business Leaders Show Low Confidence in Corporate Data Security

Global organizations are now managing a greater volume of data than ever. On average, businesses managed 9.70 petabytes of data in 2018 – up from just 1.45 petabytes in 2016, according to the Global Data Protection Index.* They are also highly aware of its value. However, these companies are challenged with properly protecting it from an ever-increasing amount of threats – from malicious cyberattacks to natural disasters to disgruntled employees.

29%

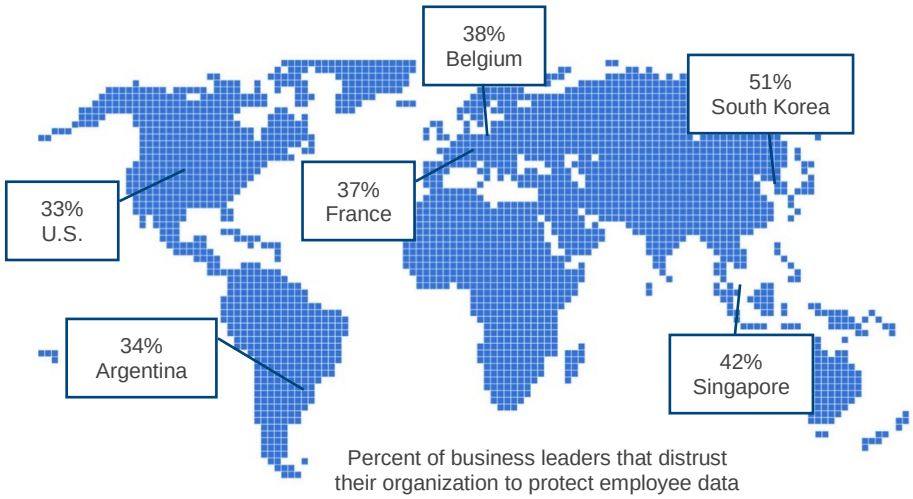
of global executives do not trust their organization to protect their data as an employee

Adding to that, global business leaders have little confidence in their companies' abilities to maintain the security and privacy of employee, business and customer information. In fact, the Dell Technologies Digital Transformation Index found that nearly one in three global business leaders (29 percent) do not trust their organization to protect their data as an employee, and even more (33 percent) said they do not trust their organization to protect customer data.† Almost half (49 percent) believe their organization will struggle to prove it's trustworthiness within the next five years.†

"Recognizing the value of data is the first step to protecting and harnessing the data that drives human progress."

Beth Phalen, President, Data Protection Division, Dell EMC

This perception circles the globe. In the Americas, 28 percent of executives are not confident in their organization's ability protect employee data from bad actors with distrust highest among business leaders in Argentina (34 percent) and the U.S. (33 percent).† The EMEA region showed a similar 28 percent rate of distrust with Belgium (38 percent) and France (37 percent) reporting the highest levels among executives.† Asia Pacific, Japan and China (APJC) showed the highest level of distrust among the regions at 33 percent with South Korea (51 percent) outpacing every other country other than Singapore (42 percent).†



Percent of business leaders that distrust their organization to protect employee data

The increased amount of data and its importance to business operations are also increasing the value of corporate data to hackers, making this lack of confidence even more alarming. In the event of a destructive cyberattack, only 35 percent of global IT decision makers are very confident that their organization could reliably recover all business-critical data and only 16 percent believe that their current data protection solutions will be able to meet all future business challenges.*

This is quickly becoming a focal point as regulation compliance was ranked in the top three data protection challenges by 41 percent of respondents.*

Moreover, only 35 percent felt very confident that their organization's current data protection infrastructure and processes are compliant with regional regulations. That sentiment is beginning to translate into reality as 12 percent of respondents whose organization experienced data loss or unplanned downtime in the past 12 months reported paying punitive fines as a result. *

This low confidence from business and IT decision makers demonstrates that organizations must make investing in future-ready data protection and privacy solutions a high priority. Yet many data breaches start from targeting individuals specifically. With a new generation entering the workforce, organizations are facing a whole new level of risk.

Gen Z Unsure of Workplace Security Best Practices

Gen Z could represent 20 percent of the global workforce by 2020, according to the Dell Technologies Gen Z Study.‡ As organizations begin to integrate these digital natives into the workforce, they must understand their unique attitudes toward security and react accordingly.

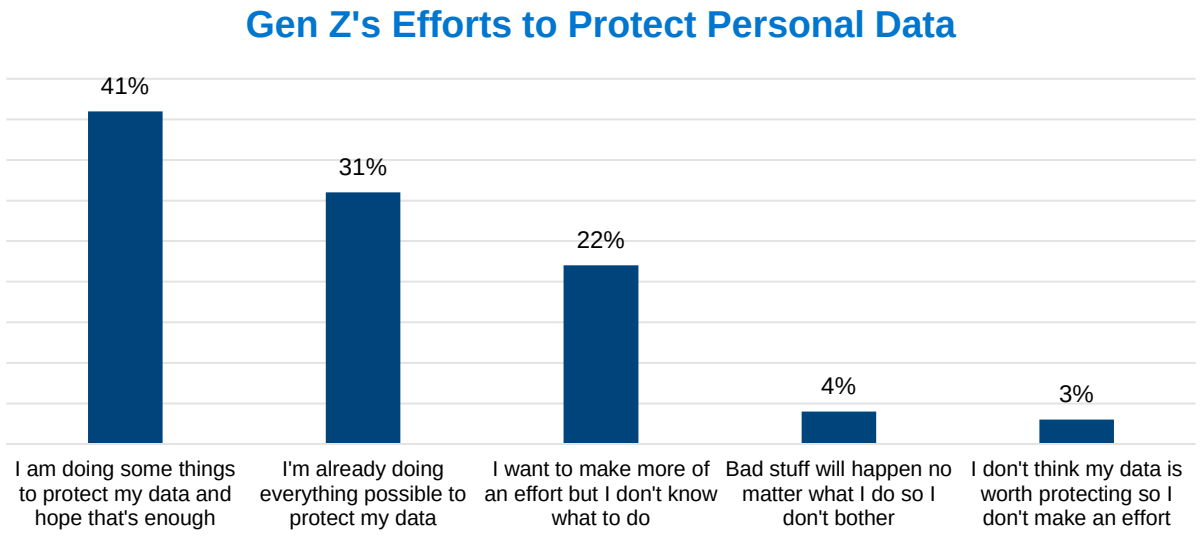
46%

of Gen Z rate their cybersecurity skills as "not good" to "just ok"

This age group is extremely tech savvy and grew up in the social media era armed with smartphones and an array of cloud-based apps. Luckily, they also understand the importance of data security. Nearly three in four Gen Zers (73 percent) globally rank their data security as a high priority, and nearly all (95 percent) are careful about what they post to social media because they believe it could impact their future careers.‡

However, many still aren't confident about the best ways to keep their data safe, which could translate to a significant risk to future employers. In fact, nearly half of Gen Z (46 percent) rate their cybersecurity skills as "not good" to "just ok."‡

However, Gen Z are interested in improving their cybersecurity skills. Twenty-two percent report wanting to make more of an effort to protect their data, but they are unsure how to address it.‡



When asked about future employers, a mere 11 percent of Gen Z think companies prioritize cybersecurity skills, and nearly two in five (39 percent) report that they want to ensure technology is used appropriately.‡ This offers a good lesson to organizations: they must prioritize cybersecurity education immediately when this generation joins the workforce.

But it's not just about teaching Gen Z cybersecurity best practices – it's also about the protection tools available to them. Luckily, Gen Z are already accustomed to biometrics, having used fingerprint readers and facial recognition technology throughout their lives on smartphones and are primed to embrace these technologies as they enter the workforce, giving them the potential to drive changes across the IT organization.

Organizations Slow to Deploy Devices with Advanced Device Security

Aside from smartphones, advanced device security features like biometric fingerprint readers, facial recognition and multifactor authentication are readily available on mainstream business laptops, offering users more secure ways to access their devices and apps than easily compromised passwords.

Without powerful security features, workers are forced to create, remember and regularly change strong passwords to access their laptops and apps. As the Dell Biometric Usage Survey found, this age-old practice is "annoying" to 88 percent of workers, causing many to exhibit poor security behavior such as writing passwords on sticky notes, using their name or meaningful numbers in passwords, or accessing personal social media accounts from corporate-issued devices.[§]

64%

of workers would use biometric security features if they had them

Interest in biometric security features is high among those who do not currently have the feature on their work PCs, with 64 percent saying they would use such features if they were available and 79 percent agreeing that having security features built into their business PCs help keep company data safe.[§]

"Security is a critical concern especially among mid-market organizations as they face myriad threats to their business assets, corporate data and customer information. They're seeing an increasing need for enterprise-grade protection without the added complexity and cost of larger-business solutions, making built-in biometric security on laptops an easy and effective choice."

Brett Hansen,
VP & GM, Client Software and Security Solutions, Dell

Businesses globally understand the benefits of strong security features, with nearly half (49 percent) reporting that they are building security and privacy into their fleets of end-user devices, applications and algorithms.[§] Notably, emerging markets (54 percent) are ahead of developed markets in this area (45 percent).[§]

However, these initiatives may be not be happening as quickly as businesses might want. Fewer than one in five full-time working adults in the U.S. (17 percent) say they currently have biometric authentication on their work PCs.[§] In the U.S., employees at mid-market businesses – those with 100 to 499 employees – have the most PCs with biometric security (23 percent), with eight in 10 (78 percent) reporting they use the feature. Comparably, although fewer staff at large businesses with more than 500 employees report having biometric security (15 percent), usage is even higher at 82 percent.[§]

Organizations can learn from these insights. As device refresh cycles arise, businesses should consider configuring technologies, like fingerprint readers, across their device deployments for enhanced security. But organizations won't reap the benefits of this advanced technology if employees don't have these features enabled and aren't educated on how to use them. Not giving employees the tools and resources they need to keep critical data secure can lead to larger problems for the organization.

Privacy and Security Concerns are Top Barrier to Digital Transformation

If organizations do not act to improve upon the overall security of their workforces, it can hamper the progress of larger, more important digital transformation initiatives that create new value such as new product and service development, increasing collaboration across business functions or investing in AI and machine learning. Globally, business executives cite data privacy and security concerns (34 percent) as the #1 barrier to their digital transformation efforts – up from #5 in a 2016 survey.[§]

When analyzing digital transformation barriers across regions, executives in APJC report that data privacy and security is the top barrier to achieving digital transformation (41 percent).[4] Among executives in the Americas and EMEA, that sentiment was not felt as strongly, both dropping it to their #2 concern (Americas 29 percent and EMEA 31 percent) just behind lack of budget and resources.[§]

#1

Global barrier to digital transformation are Data Privacy & Security Concerns

This concern is not going unnoticed. Business leaders are taking note with the majority (58 percent) of respondents claiming that cybersecurity will be their top investment over the next one to three years as a key pillar to enable their digital business.[§] However, most businesses remain behind the curve with nearly eight in 10 (78 percent) business leaders admitting digital transformation should be more widespread throughout their organization, and more than half (51 percent) believing that they'll struggle to meet changing customer demands within five years.[§]

Final Takeaways

With the progress of digital transformation initiatives at risk and a severe uptick in data breaches across every industry, we are at a critical point where organizations can either act or face dangerous repercussions that can affect their businesses for years to come. To overcome the challenges security issues pose, organizations must employ a multi-pronged approach that encompasses data protection solutions, security education and training, protected devices, and secure solutions that enable digital transformation. By taking a multipronged approach to security in the workplace, organizations can empower and enable their workforces to be their most productive without interfering with workflows.

- Subscribe value to data and protect it accordingly. Develop clear policies and guidelines that define end-user data access, types of data and rules for its dissemination outside of the organization. As data continues to grow exponentially, it is essential to leverage a variety of data protection strategies across continuous availability, replication, backup, archives, etc. creating an effective data protection solution that can scale.

- Provide security training to all staff and reinforce it. It is critical that all employees understand why data security is critical at every level and how they are an important part of keeping it secure whether they're on the clock or off. Educate staff about common and unexpected scenarios where data can be compromised and how they can exhibit better security behaviors. Such trainings should begin in the onboarding process and be regularly reinforced to mitigate complacency.

- Utilize built-in security technologies. Modern business laptops can easily be equipped with fingerprint readers, smart card readers and facial recognition technology that can ease the burden of creating and updating strong passwords. Deploy integrated security features wherever available, especially as device refresh cycles arise.

- Balance advanced security and encryption with productivity. To be productive, workers need easy-to-use solutions that help them get their work done, but overly complicated security measures can be a barrier, causing them to find workarounds and opening up vulnerabilities. Look for solutions that don't force a trade-off. Instead, look for ones that give a high level of assurance, while enabling end users to work more freely. In addition, regularly pulse employees to understand what obstacles they're facing and find solutions to adapt to their needs.

Survey Methodologies

* **Dell EMC Global Data Protection Index**
Dell EMC commissioned Vanson Bourne for the third Global Data Protection Index, surveying 2,200 IT decision makers from both public and private companies with 250+ employees across 11 industries and 18 countries about the maturity of their data protection strategies. Vanson Bourne conducted the survey between September and November 2018. The countries surveyed include US, UK, France and Germany with 200 respondents each, and Canada, Mexico, Brazil, South Africa, UAE, Italy, Switzerland, Netherlands, Australia, Japan, China, South Korea, India and Singapore with 100 respondents each.

† **Dell Technologies Digital Transformation Index**
During the summer of 2018, independent research company Vanson Bourne surveyed 4,600 business leaders from mid- to large-size companies across 42 countries/sub-regions to gauge their organizations' place on the Dell Technologies Digital Transformation Index. Vanson Bourne classified businesses' digital business efforts by examining their IT strategy, workforce transformation initiatives and perceived performance against a core set of digital business attributes.

‡ **Dell Technologies Gen Z Study**
This study was commissioned by Dell Technologies and undertaken by an independent research firm. From August to September 2018, Dimensional Research conducted an online survey of students attending secondary and post-secondary school in 17 countries around the globe. The survey was translated into 12 languages and more than 12,000 individuals aged 16-23 completed the survey. The study is one of the largest of its kind to gather hard data on current attitudes and opinions on technology and the workplace among Generation Z students who will be entering the workforce in the coming years.

§ **Dell Biometric Usage Survey**
Dell commissioned Ipsos who conducted an online poll from March 22–26, 2019 among 1,050 adults ages 18 and over from the continental U.S., Alaska and Hawaii. To qualify for the survey, respondents had to be employed full-time. The precision of Ipsos online polls is measured using a credibility interval. In this case, the poll has a credibility interval of ±3.4 percentage points for all respondents.

About Dell Technologies

Dell Technologies (NYSE:DELL) is a unique family of businesses that helps organizations and individuals build their digital future and transform how they work and live. The company provides customers with the industry's broadest and most innovative technology and services portfolio spanning from edge to core to cloud. The Dell Technologies family includes Dell, Dell EMC, Pivotal, RSA, Secureworks, Virtustream and VMware.