Centrify®
ZERO TRUST SECURITY

SECURITY, PRIVACY AND THE NEXT-GENERATION WORKFORCE

US +1 (669) 444 5200 | EMEA +44 (0) 1344 317950 | Asia Pacific +61 1300 795 789
Brazil +55 11 3958 4876 | Latin America +1 305 900 5354 | sales@centrify.com

Executive Summary

The age gap has been a perennial theme for hundreds of years. Generations of parents have shrugged in bewilderment at younger peoples' music, fashions and pastimes, and sometimes blamed them for the impending collapse of society. Now, these attitudes are drifting into the workplace. Senior managers are finding it harder to understand the next-generation workforce, which is making it difficult to assess and guide attitudes to security and privacy at the office.

Centrify set out to measure what managers think of the next generation workforce's approach to security and to compare it to real-world attitudes and practices. Working with UK survey group Censuswide, it interviewed 1,000 UK office workers aged 18-24 (confidence interval: 3.1) and 500 senior decision makers (confidence interval: 4.38). It spoke only to those who spent at least 25% of their time in the office, and excluded sole traders.

The research highlighted several areas of concern among senior decision makers, but also gave us a unique insight into the real-world attitudes and activities of younger employees in the workplace. This enabled us to sanity check those management concerns and see which were valid. We found a significant gap between perception and reality in managers' views of younger workers, along with a lack of action among senior decision makers to fix cybersecurity problems within their organisations.

Based on this research, Centrify has been able to identify some key recommendations that senior decision makers can follow to help bridge the gap and harmonise approaches to data security and privacy in the workplace.

Introduction

They are tech-savvy, adventurous, and hooked on social media. They are already in your office, and in ten years' time, they will form 75% of the workforce. Next-generation workers aged 18-24 are the future of your company, yet most decision makers have a negative view of them, viewing them as a security risk and arguing that their attitudes must change.

Managers Blame Younger Workers for Security Problems

One data point that stood out in Centrify's survey was executive concern around younger employees' security consciousness.

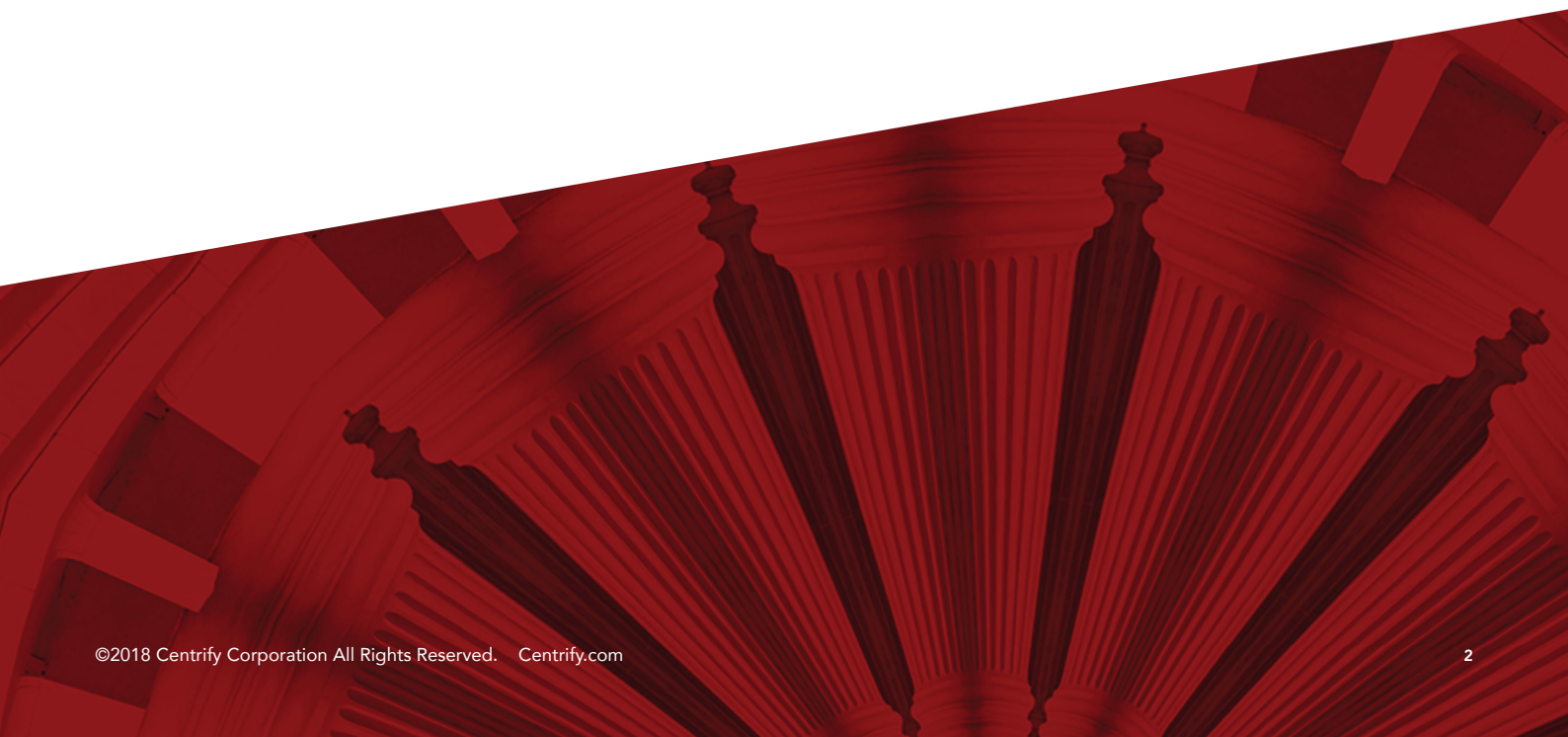
Over one third of decision makers (35%) believe that younger employees are mostly to blame for workplace data breaches. 37% of decision makers said that younger workers are too relaxed about security measures.

In general, decision makers would like to see younger people share information and trust in technology a little less and be more patient. 35% of managers were concerned that younger workers placed too much trust in technology. 30% said that they shared data too easily, and 22% said that they were most worried that next-generation workers expected immediate access to data.

Social Media is a Weak Spot

When they do want to share, social media is the channel of choice for next-generation workers, and this stood out as a risk factor that worried decision makers. Media stories about employees endangering brand reputation with inappropriate posts have obviously had an effect. 48% of senior executives worried about how younger workers interact on these highly visible networks.

These concerns are well-founded. Today's next-generation workforce is addicted to social media, with 13% regularly logging in and posting personal updates on social media while at work. The survey showed that 21% of younger workers do not worry about how their social media activity might affect their employers, and 18% freely admitted that their posts could compromise security.



Misuse of Technology

Among decision makers, the biggest concern about next-generation workers was that they would misuse technology – 44% of managers believed this

The top concern for 67% of managers was employees clicking on a suspicious link or email. Followed by employees removing information from the company by saving it to a USB key or sending it to their own email, for example, with 58% of decision makers worried about this.

In practice, actions by younger employees did not really reflect those concerns. Only one in 10 workers in the 18–24 age group had clicked on a suspicious link, and only 7% had removed information from the company.

By far the biggest infraction that younger workers admitted to was sharing passwords.

16% said that they had shared passwords with colleagues while 13% said that they had done so with managers

This was in the top three concerns for decision makers', with 56% worried about this issue.

In some cases, managers are nearly as likely and sometimes more likely to misuse technology as younger workers. 15% of managers admitted to sharing passwords with colleagues. More decision makers (5%) than younger workers (2%) had been on the dark web, downloaded hacking tools or sent ransomware to someone.

At 18%, almost twice as many managers had clicked on a suspicious link compared to younger workers. This is paradoxical, given that managers saw malware as the single biggest security risk to their organisations (24%).

Managers' failures to lead by example were numerous. At 15%, more than twice as many managers had removed information from the company, while 14% had logged onto a risky website, compared to 7% of those in the next-generation workforce.

The same disparity extended into personal device usage – 38% of decision makers worried about younger workers co-opting work devices for personal use, yet more of them played games on work devices (18%) than younger workers (15%)! Around one in eight (12%) of decision makers used devices for online gambling, compared to 1 in 20 (5%) younger workers, while 6% of managers watched porn and sent sexual texts from mobile devices, compared to 2% of employees aged 18-24.

This shows us that decision makers are not practicing what they preach. Leading by example is an important part of any organised security awareness program, but survey findings show that in many cases, managers are more guilty of risky behaviour with work devices than those they are supposed to be mentoring.

Security Policies

A failure to lead by example is not the only area where decision makers need more work.

Many are still failing to create and communicate policies governing information security and appropriate use of workplace resources

84% of decision makers said that they actively raise awareness about security among employees, and almost all of those (83%) said that there were disciplinary consequences for those that failed to follow security stipulations. Only slightly fewer – 80% – agreed that they have a robust security policy in place.

In practice, it can be difficult getting employees to comply. Nearly three-quarters (74%) of decision makers agreed that employees abide by their security policies. This aligns with the 75% of younger workers that said they are aware of security policies at work – and always stick to them.

These numbers are promising, but still leave room for improvement.

One in five companies is failing to provide next-generation workers with clear guidelines on basic security issues such as appropriate use of workplace devices and management of data

Communication and enforcement could also be better; one in four younger workers are not following security guidelines strictly, leaving companies vulnerable.

The scope of these security policies is also narrow, at a time when the number of risk vectors is growing. When asked whether they had guidelines in place to deal with employees who accessed the dark web, underground hacking forums or crimeware, fewer than half (48%) of decision makers said that they had strict guidelines. Another 40% said that they had guidelines, but that they could be better, implying that security policies need to move more quickly to keep up with evolving threats.

Social media stood out here as an area in need of attention. Just 40% of young people said that their employers have clear guidelines around social media usage, which helps to explain the laissez-faire attitude towards social media at work among this age group.

Decision makers were aware of this and understand that it poses a significant risk. One third of them worried about the next generation workforce's failure to comply with security policies, making it the second most-likely way in which young people could negatively affect the workplace, according to senior management.

Few Controls in Place

The modern workplace cannot rely on policies alone to enforce security. Even surveillance will not suffice. Over a third (35%) of younger workers know that employers monitor their work devices remotely but said that it does not change their online behaviour. It is not enough to watch what employees are doing; technical controls provide a valuable means of enforcing security procedures and keeping data safe.

Unfortunately, these controls are lacking in the modern workplace, and despite their worries around next-generation workforce security issues, managers do little to protect themselves.

Around one in three (36%) of younger employees can access any files on their business networks

Only one in five (20%) must request permission to access specific files, and only 43% are restricted to accessing files and data relevant to them. This leaves a large proportion of younger workers with free access to data, and yet only 58% of managers worry about them taking company information away from the workplace.

While over half (56%) of all managers highlighted password sharing as one of their biggest security concerns, password management controls are not much better. 6% of younger workers do not follow their employer's policy when it comes to setting their password, and many freely share passwords with each other.

Many companies are not mitigating the problem with appropriate measures, such as regular password changes.

Only 40% of employers enforce a regular password change according to younger workers

29% of next-generation workers are completely in control of when they change their passwords, and 14% have been using the same password for over a year on their work device.

Perhaps most worrying is the 14% of respondents that use the same password across both their work and personal devices

One thing that would mitigate this password problem is two-factor authentication (2FA). This technique requires a user to enter a code tied to their physical device (typically their phone) before gaining access to a system. However, adoption is low, with just 11% of younger workers required to use it. In fact, one in ten need no username or password at all.

Who is Responsible for Cybersecurity?

In any successful cybersecurity initiative, everyone shares responsibility to secure company resources. Employers have a responsibility to set security policies and lead by example, and to put controls in place that enforce those policies. Employees have a responsibility to follow those guidelines and think carefully about their use of company resources.

In practice, decision managers and younger employees are not working together as a team. While senior managers fail to put controls in place, less than half (48%) of the next-generation workforce took partial responsibility for their role in online security and privacy at work, although another 12% took complete ownership of the issue.

Among those that assigned responsibility entirely or partly elsewhere, 44% placed it on the IT department, and more than one in five (21%) said that it was the boss's job.

These numbers show a significant proportion of younger workers are unwilling to accept any responsibility for security and reveals a gap in business security that decision makers must address.

Closing the Gap

Closing the gap between senior managers and the next-generation workforce may be difficult. We noticed several statistics that highlighted the need for more work in bridging this gap.

Understanding

Only 39% of decision makers are sure that they are doing enough to understand younger workers.

Leadership

Over half (52%) of managers tend to follow their security policies properly, yet only 12% of decision makers think that senior managers are the main cause of the problem. We must lead by example.

Communication

79% of decision makers say that they regularly circulate communications to ensure employees stick to security polices. That is a promising figure, but with one in five senior managers not communicating with employees on security, that leaves significant room for improvement.

Conclusion

Managers' assumptions that next-generation workers are the root of cybersecurity problems in the workplace may be overstated, but there are some areas, such as social media use and password management, where younger workers do need extra mentoring. Decision makers can do more to address this problem by putting technical controls in place, refining security policies and communicating them effectively to employees. Equally important is leadership and the need for decision makers to set a good example. If managers can demonstrate a commitment to security through their own policies and actions, then the next-generation workforce will surely follow.

Research Methodology

The statistics cited in this report are from two separate surveys for Centrify conducted in May 2018 by Censuswide via an online questionnaire of:

- 1,000 UK office workers aged 18-24 who spend at least 25% of their time in the office.
- 500 UK Senior Decision Makers (exc. sole traders) who spend at least 25% of their time in the office.

Censuswide abides by and employ members of the Market Research Society, which is based on the ESOMAR principles.

About Centrify

Centrify delivers Zero Trust Security through the power of Next-Gen Access. The Centrify Zero Trust Security model assumes that users inside a network are no more trustworthy than those outside the network. Centrify verifies every user, validates their devices, and limits access and privilege. Centrify also utilizes machine learning to discover risky user behavior and apply conditional access — without impacting user experience. Centrify's Next-Gen Access is the only industry-recognized solution that uniquely converges Identity-as-a Service (IDaaS), enterprise mobility management (EMM) and privileged access management (PAM). Over 5,000 worldwide organisations, including over half the Fortune 100, trust Centrify to proactively secure their businesses.