SAFETY FIRST:

THE FACE OF CYBERSECURITY IN TODAY'S WORKPLACE

As working environments and styles change, organizations must adapt IT to keep devices secure.

Contents

51%
of employees want more flexibility in working practices.[3]

Welcome to the modern workplace

The digital revolution has altered every aspect of modern life, and the way people work is no exception. Today's workplace would be unrecognizable to the average worker of the past. In fact, the modern work environment has transformed substantially in the last 10 years alone, and the revolution in the way people work means IT faces more complexity than ever before.

Employees are no longer viewing the traditional 9 to 5 day as the norm, with almost two thirds of workers valuing work-life balance over salary.[1] As the popularity of flexible working rises across different sectors,[2] what was once confined to an office can now be completed from home, from off-site locations, on the go and even from the other side of the world.

The shift in routines bring changes to the way employees access devices. Where computers used to be practically tethered to office spaces, employees now regularly work from their own devices, including smartphones and tablets. This can mean work-related tasks are carried out on unsecured devices, with 60% of personal devices not being monitored for security.[4] The BYOD security global market is expected to grow to approximately $69 billion by 2023, at 37% of CAGR between 2019 and 2023.[5]

Although this increased flexibility makes it easier and more convenient for employees to manage workloads, for IT, "easy" isn't exactly the word that comes to mind.

Millennials already comprise

35%

of the US workforce.[6]

Digital natives are leading the tech revolution

Many factors are driving workplace fragmentation. For one, as baby boomers age into retirement and millennials take their place, the number of digital natives – people who have grown up in a world where the internet, social media and smart devices are ubiquitous – in the workforce is multiplying swiftly. Millennials (also called Generation Y) are typically defined as those born in the 1980s and early '90s. According to the latest population estimates from U.S. Census Bureau, millennials have already overtaken baby boomers, comprising more than one of three adult Americans – the largest generation in the US workforce.[6] Globally, the figures look the same, the digital-savvy generation account for a quarter of the population[7] and have high expectations for the devices and tools they use at work, with many banking on the same accessibility and flexibility they're used to in their personal lives.

Generation Z – the first fully digital generation – are following millennials into the workplace in large numbers, accounting for 61 million of the US population.[8] On top of this, 95% of teens now report to have access to a smartphone and almost half are online on a near-constant basis.[9] Once digital natives dominate the workforce, organizations will have to adapt the way they operate to meet new expectations.

As the changing workforce puts pressure on companies to adopt the use of mobile and personal devices, significant business trends, such as data analytics, the digitization of business functions and the blending of service offerings across industries, are also expanding the use of technologies. This expansion increases the boundaries of what's possible, and it also creates risks.

At the rate technology is evolving, there's no time to waste. It's critical that organizations invest in solutions to not only move business forward but also protect against rising threats such as cybercrime. To meet this objective head-on, IT must adapt to become more agile and proactive.

The decentralized workplace is a double-edged sword

The workplace of today, decentralized and always on, presents several challenges for IT, but it also offers opportunities. The surge in complexity has transformed tasks that used to be simple, such as updating an operating system, into multilayered undertakings. Plus, the number of devices IT must manage and secure is rising with no sign of slowing down. By some estimates, devices are projected to outnumber humans by almost four-to-one by the year 2022.[10]

As the technology for which IT is responsible becomes increasingly complex, resources will grow strained as time spent managing endpoints and supporting users competes with the need to deliver on strategic IT initiatives. Moreover, there is a distinct lack of skilled professionals to tackle the growing IT demand, with an estimated global shortfall of over 2 million. And organizations are feeling the strain, as lack of personnel has become the top job concern for the cybersecurity sector.[11]

IT leaders can leverage their institutional knowledge to become valued strategists, influencers and stakeholders within their organizations.

Workplace technologies have become a differentiator for many businesses, and that means IT leaders play an influential role in enterprise innovation and growth. Companies that use new technology – and offer the flexibility it can provide – will attract employees and prospects. Additionally, technology is being used more and more to inform major business decisions. As a result, IT is stepping out from behind the help desk. Instead of simply managing the technology that's currently in use, IT leaders can leverage their institutional knowledge to become valued strategists, influencers and stakeholders within their organizations.

Security is a moving target

As every other aspect of business goes digital, it should come as no surprise that crime has too. Cybercrime continues to evolve and become increasingly sophisticated every day. From 2016 to 2018, almost a third of organizations were a victim of cybercrime. What's more, cybercrime has grown to be the second most reported frauds affecting organizations (behind misappropriation), and is more than twice as likely to be identified as the most disruptive and serious economic crime over the next two years.[12]

In November 2018, Marriott announced that its Starwood Hotel brand was subject to a data breach, which exposed personal information of up to 500 million customers – going back four years to 2014. Following reports of the breach, which compromised details such as names, addresses and passport numbers, the multinational hospitality company's stock fell by 5.6%.[13]

With high profile breaches hitting the headlines over the last couple of years, it's critical that organizations have the right measures in place to safeguard personal data. To protect their citizens, the European Union has standardized policies with the General Data Protection Regulation (GDPR), which went into effect in the European Union in May 2018.[14]

Cybercrime is escalating and organizations are becoming more vulnerable because of the hyperglobalization of business. However, many business leaders fail to think of the security risks that come with remote collaboration, perhaps because constant connectivity has become such a mainstay in modern life. The threat of cybercrime and the pressure on IT to keep devices secure will only continue to rise. To thwart costly risks, it's crucial that IT avoid becoming bogged down in a reactionary way of responding to threats.

Top reported types of economic crime[12]

45% asset misappropriation

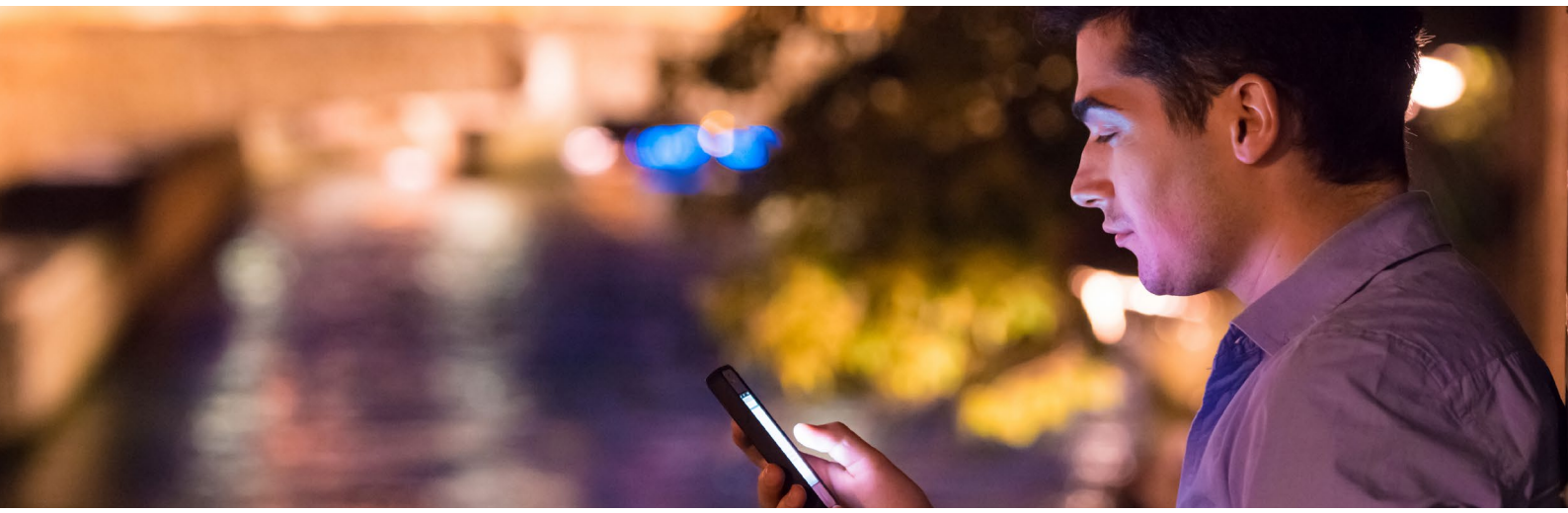
31% cybercrime

29% consumer fraud

The cost of cybercrime goes beyond dollars and cents

A recent study by the Ponemon Institute, an independent research firm, found that, on average, a security breach can cost companies nearly $4 million – up 6.4% from 2017 – and in the US, the cost is even higher, at $7.9 million.[15] While these figures are concerning, the simple economic cost of cybercrime doesn't tell the full story. For one thing, cybercrime costs organizations time and resources. The average time it takes to contain a data breach is 69 days.[15]

The negative impacts of cybercrime can be more difficult to quantify. A global survey conducted by the multinational professional services network PwC found that employee morale and business relations were the top forms of damage caused by cybercrime.[12] Both of these areas deal with relationships: internal relationships (employee morale) and external relationships (business relations), which indicates that maintaining a reputation is a major concern for organizations. It's important for IT to keep this type of intangible damage in mind when assessing risk, as repairing a reputation can be more difficult than recovering from economic losses.



A modern service model can help IT stay on top of security needs

IT leaders spend a great deal of their time ensuring software is up to date and devices are secure. Imagine what leaders could accomplish with additional time to devote to strategic IT initiatives. Rather than working in a constant cycle of alerts and responses, IT could be more proactive and forward thinking, to the benefit of the whole business.

One way to relieve the burden of daily tasks is to take advantage of Device as a Service (DaaS). A modern service model, DaaS simplifies how organizations equip users with the right devices, accessories and lifecycle services while improving efficiency and cost predictability for IT. The DaaS model enables organizations to more easily keep assets up to date, better manage IT spending, maximize resources and strengthen security positioning. It also provides the flexibility businesses need by offering adjustable agreements to match workloads and optimize IT budgets. The predictability of one price per device greatly simplifies the process of purchasing computing solutions.

With the HP DaaS model, organizations do more than purchase a device; they enter into a strategic relationship with their device provider and can gain access to powerful, insightful and actionable analytics that help to address issues before they become a problem. Organizations will be supported with:

- The latest OS updates and patches to minimize security vulnerabilities and keep devices up to date
- Enforcing security configuration and encryption policy settings*
- Device security incident reports
- Data protection on missing devices†
- Securely provisioning Wi-Fi to end users
- Real-time protection against threats through browsers, email, files and human error‡
- Proactive security threat analysis
- Predictive analytics for Windows, Android™ and Mac devices§

47%

of IT professionals spend more than 4 hours a day addressing security alerts[15]

Learn more about what DaaS can do for your business

Changing workforce demographics and advances in technology have created a work environment that's increasingly vulnerable to the threat of cybercrime. IT leaders must manage and secure a decentralized workplace while, at the same time, evolve into their roles as strategists and stakeholders within their organizations. DaaS can enable IT to manage growing complexities and help propel enterprises into a new era of innovation and collaboration.

Learn more about HP DaaS

*Security Policy and Enforcement and Lock and Wipe available on HP DaaS Enhanced or Premium plans only.
†Remote lock and wipe functionality requires the device to be powered on and have Internet access.
‡HP DaaS Proactive Security Service available as a separate purchase for Windows 10 devices, regardless of manufacturer. See www.hpdaas.com/requirements for additional system requirements. The HP DaaS Proactive Security Service requires HP TechPulse, which is included in any HP DaaS or HP DaaS Proactive Management plan. Security Experts available in the Proactive Security Enhanced plan only.
§For full system requirements, visit www.hpdaas.com/requirements. iOS devices are not covered in the Standard plan.

Sources

1. Business Opportunities, Attitudes towards flexible working are changing worldwide, January 2019.
2. Marketing Week, Salary Survey 2019: Flexible working and career breaks, January 2019.
3. Mercer, 2018: Mercer's 2018 Global Talent Study: Unlocking Growth in the Human Age.
4. HR Dive, Employees use personal devices for work without much oversight, May 2018.
5. Market watch, BOYD security global market report 2019, March 2019.
6. Pew Research, Millennials are the largest generation in the U.S., April 2018, labor force.
7. FT, The millennial moment - in charts, 2018.
8. CNBC, 61 million Gen Zers are about to enter the US workforce and radically change it forever, May 2, 2018.
9. Pew Research, Teens, Social Media & Technology 2018, May 2018.
10. Cisco, Visual Networking Index: Forecast and Trends, 2017–2022, February 2019.
11. ISC2, Cybersecurity professionals focus on developing new skills as workforce gap widens, 2018.
12. PwC, Pulling fraud out the shadows: Global economic crime and fraud survey, 2018.
13. Forbes, Marriott Breach Exposes Far More Than Just Data, December 4, 2018.
14. EU GDPR portal, (accessed 04 March 2019).
15. IBM, 2018 Cost of a Data Breach Study by Ponemon, 2018.
16. Imperva, Survey: 27 percent of IT professionals receive more than 1 million security alerts daily, May 2018.

4AA7-2224ENW, April 2019