



The changing shape of ransomware

**How to defend against and respond
to ransomware attacks**

KPMG International

home.kpmg/cybersecurity



Foreword

There has never been a catalyst for technological and digital change like COVID-19.

Prior to the pandemic, video conferencing tools were only used by a niche few. Homeworkers were those that had managed to 'make it work.'

Today, communicating remotely is the norm; 86 percent of businesses have moved a significant percentage of their workforce to remote working.¹ This trend won't change anytime soon, with only one-third (31 percent) of CEOs anticipating a return to normal in 2021 and nearly half (45 percent) expecting normality to resume in 2022. Significantly, 24 percent of leaders say that their business has changed forever.²

With this new way of working comes increased risk. Since the start of the pandemic, cyber criminals around the world have capitalized on this disruption. They have further industrialized the scale at which they can launch attacks. At the top of the list, offering quick returns, is ransomware.

At a time when many can't afford to suffer any business disruption, we see an increase in cyber security threats. 41 percent of organizations have reported experiencing increased incidents while employees are working from home.³

With remote working set to continue, it is more critical than ever that organizations protect themselves and their people from attacks — but how?

In *The changing shape of ransomware*, we explore ransomware's increasing threats and identify the proactive and reactive measures to take to defend against such attacks and respond if the worst should happen.

Edward Goings
Global Incident Response
Lead and Principal
KPMG in the US



¹ Harvey Nash/KPMG CIO Survey, 2020.

² KPMG's CEO Outlook Pulse Survey, 2021.

³⁻⁴ Harvey Nash/KPMG CIO Survey, 2020.

⁵ Sophos Whitepaper, May 2020.

⁶⁻⁷ H1 2020 Cyber Insurance Claims Report, Coalition Inc., 2020



Ransomware:/'rans(ə)mwɛ:/

A type of malicious software designed to block access to a computer system until a sum of money is paid.

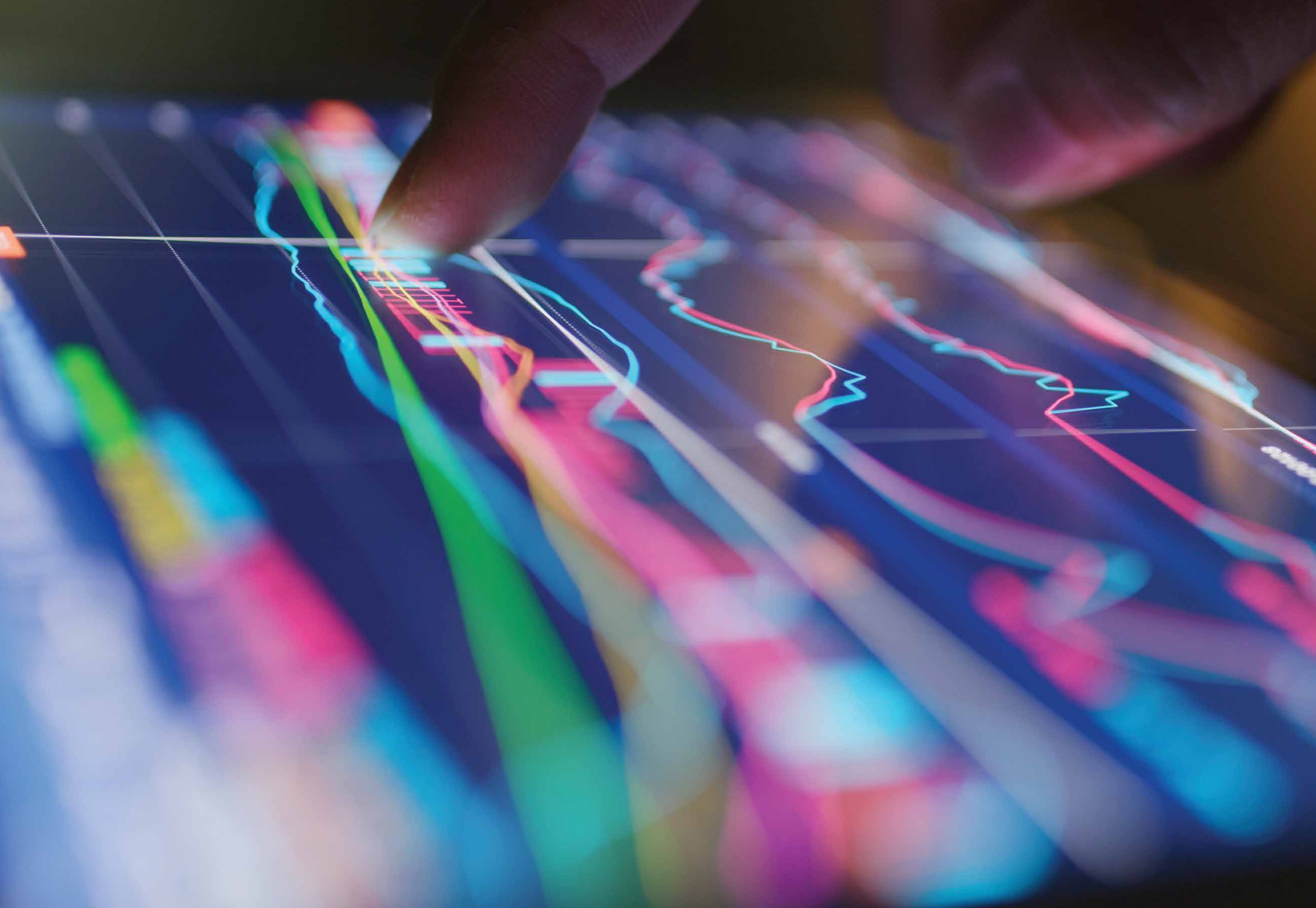
41% of reported attacks had ransomware accounts⁴

51% of companies said they had a ransomware incident in the last year⁵



100% increase in the average ransom demand from 2019 to Q1 2020⁶

47% further increase in the first 6 months of 2020⁷



Contents

Ransomware then and now	06
Adapting to the changing shape of ransomware	08
Preparing for an attack — a proactive approach	09
Responding quickly to an attack — a reactive approach	11
Staying on top of ransomware	13
About KPMG	14

Ransomware then and now

Ransomware first gained global notoriety as a result of the WannaCry attack in 2017. This campaign was unprecedented in scale according to Europol,⁸ which estimates that around 200,000 computers were infected across 150 countries. One major target was the National Health Service in England, with 80 of the 236 health care trusts impacted. Thirty-four of these trusts and over 600 other primary care organizations had active infections causing computers to be locked, including MRI scanners, blood storage refrigerators and theatre equipment.⁹

Where ransomware attacks are successful, the costs can be substantial:

- **Tangible costs** include loss of revenue while systems are down, the cost of remediation and customer compensation or litigation. Some companies may choose to pay the ransom, but that doesn't always result in the data or systems being released.
- **Intangible costs** are harder to measure but include loss of reputation. In the worst cases, it could have even more impact long-term if trust is damaged.

COVID-19, lockdown and a massive shift to remote working have seen a meteoric rise in ransomware incidents.¹⁰ Vulnerabilities in people, process and technology controls, due to a move to remote working over this period, have presented huge opportunities for cyber criminals.

Attackers can use many different methods to get ransomware onto systems, making it difficult to defend against these threats.

For ransomware to function as intended, it must be delivered, like a virus, to its host. In this case, the host is your network and systems. To get the ransomware onto your system, attackers are looking for network vulnerabilities they can exploit. Since COVID-19 has increased the number of employees working from home, the risk has increased.



⁸ "Cyber-attack: Europol says it was unprecedented in scale" BBC News. 13 May 2017.

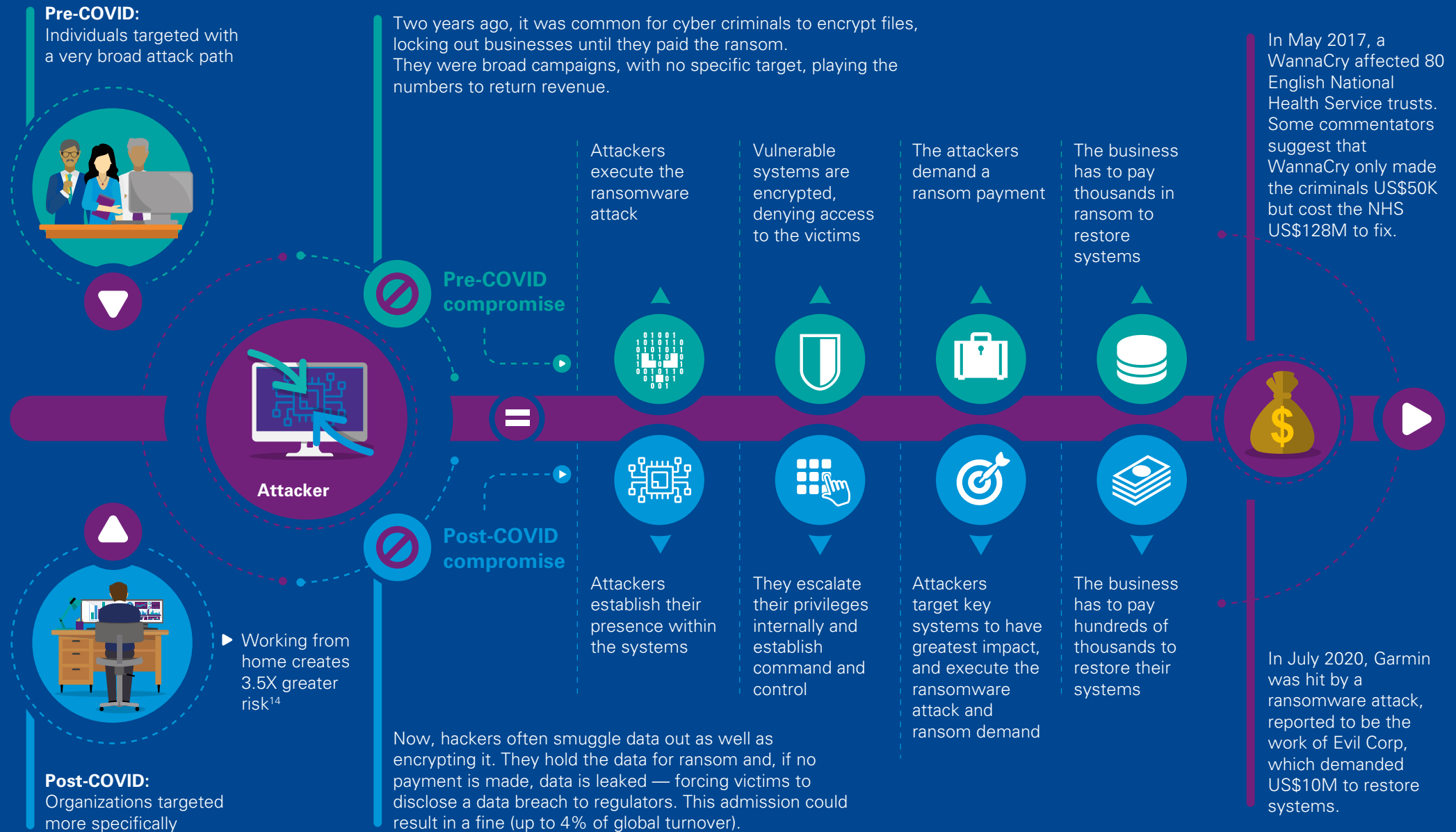
⁹ National Audit Office, Investigation: WannaCry cyber attack and the NHS, April 2018.

¹⁰ Harvey Nash/KPMG CIO Survey, 2020.

¹¹ H1 2020 Cyber Insurance Claims Report, Coalition Inc., 2020.

¹²⁻¹³ Sophos Whitepaper, May 2020.

How attacks have changed as a result of COVID-19

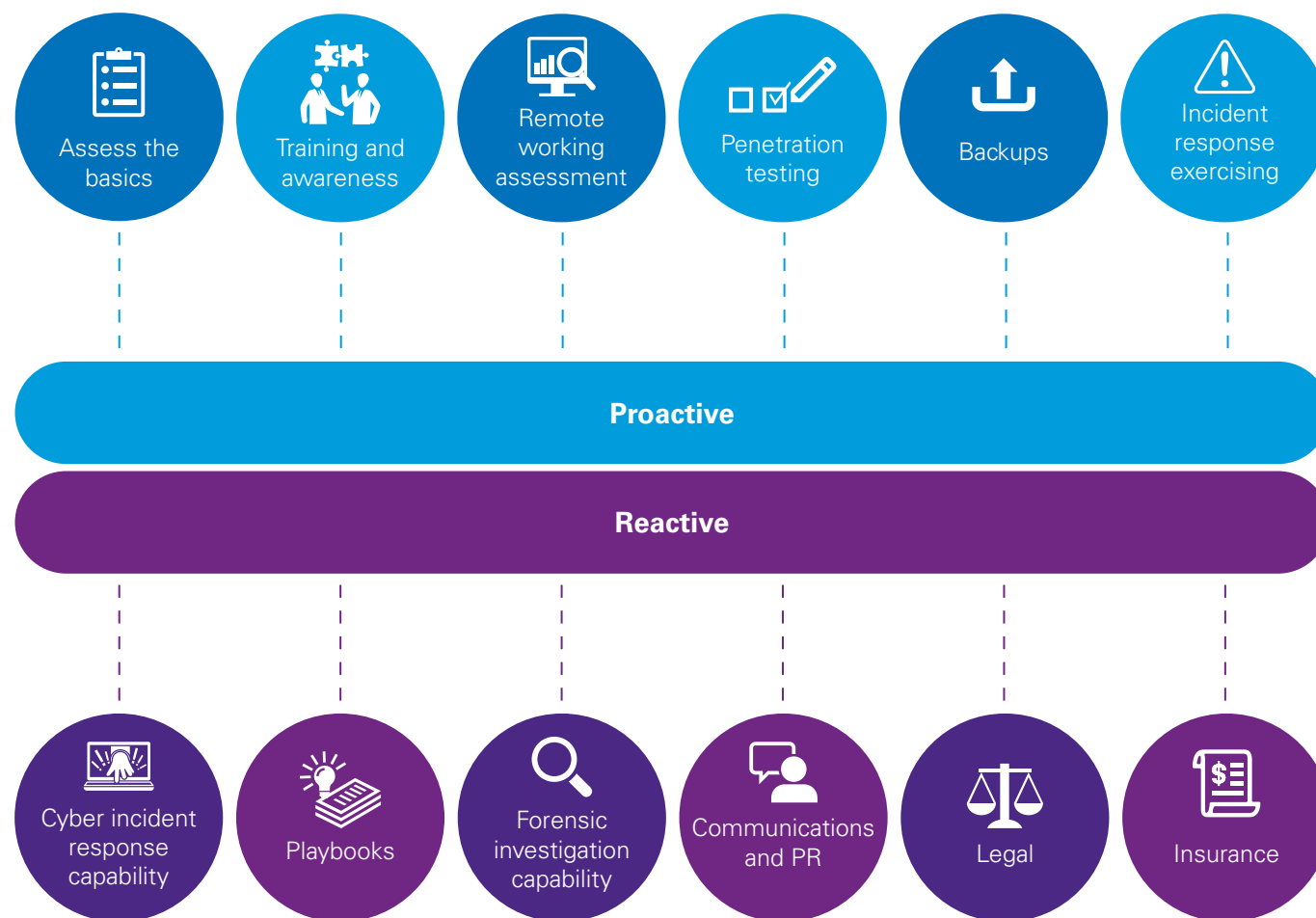


¹⁴ Identifying Unique Risks of Work from Home Remote Office Networks, Bitsight Blog, April 14, 2020.

Adapting to the changing shape of ransomware

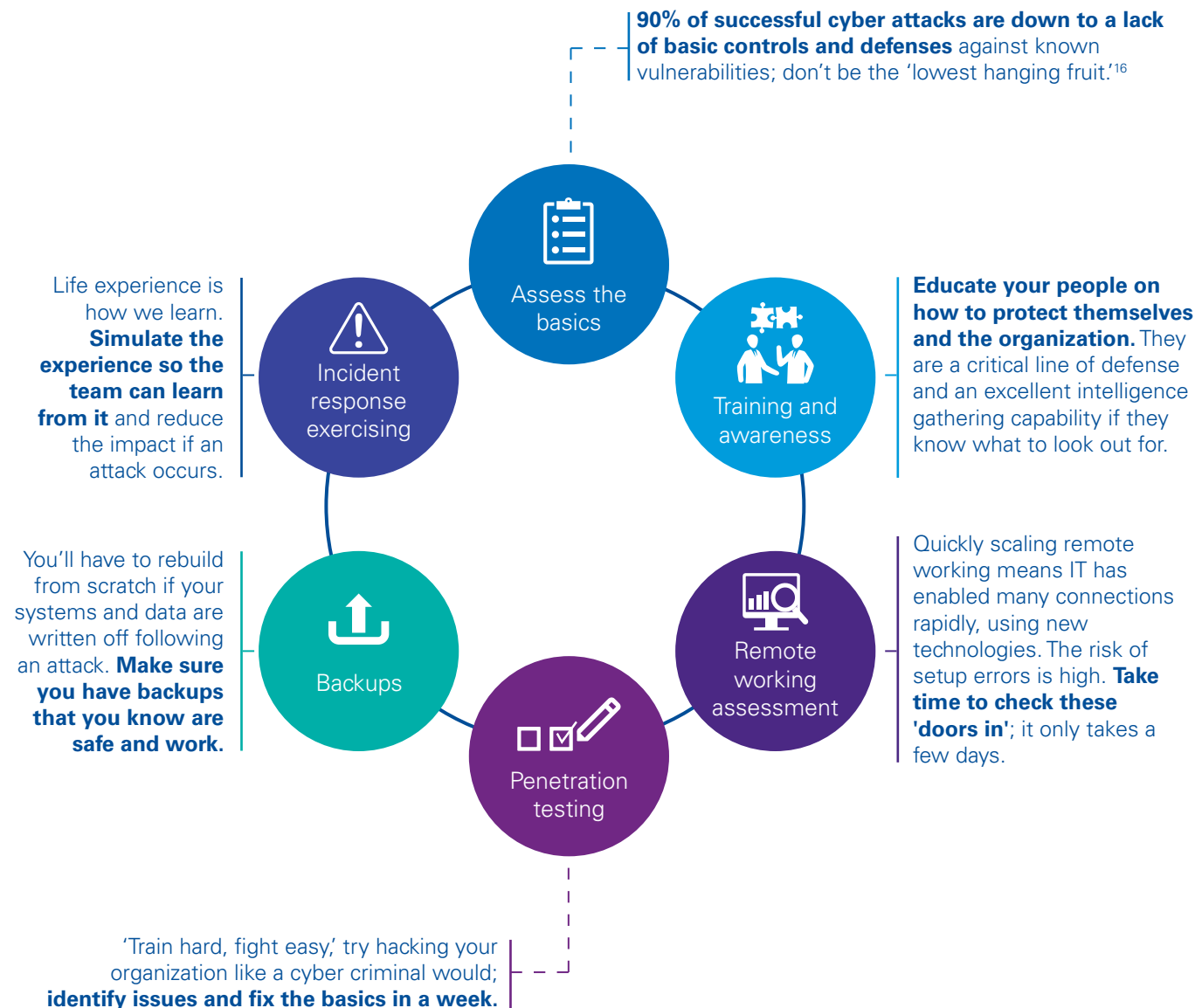
85-90% of ransomware campaigns work by targeting known vulnerabilities to gain initial access.¹⁵ These are existing issues or gaps in IT systems for which a fix is known — indicating that much more can be done to combat the threat proactively.

However, if a ransomware attack is successful, reactive steps can be taken to reduce impact and minimize business disruption.









¹⁵ Verizon 2020 data breach report

Preparing for an attack — a proactive approach

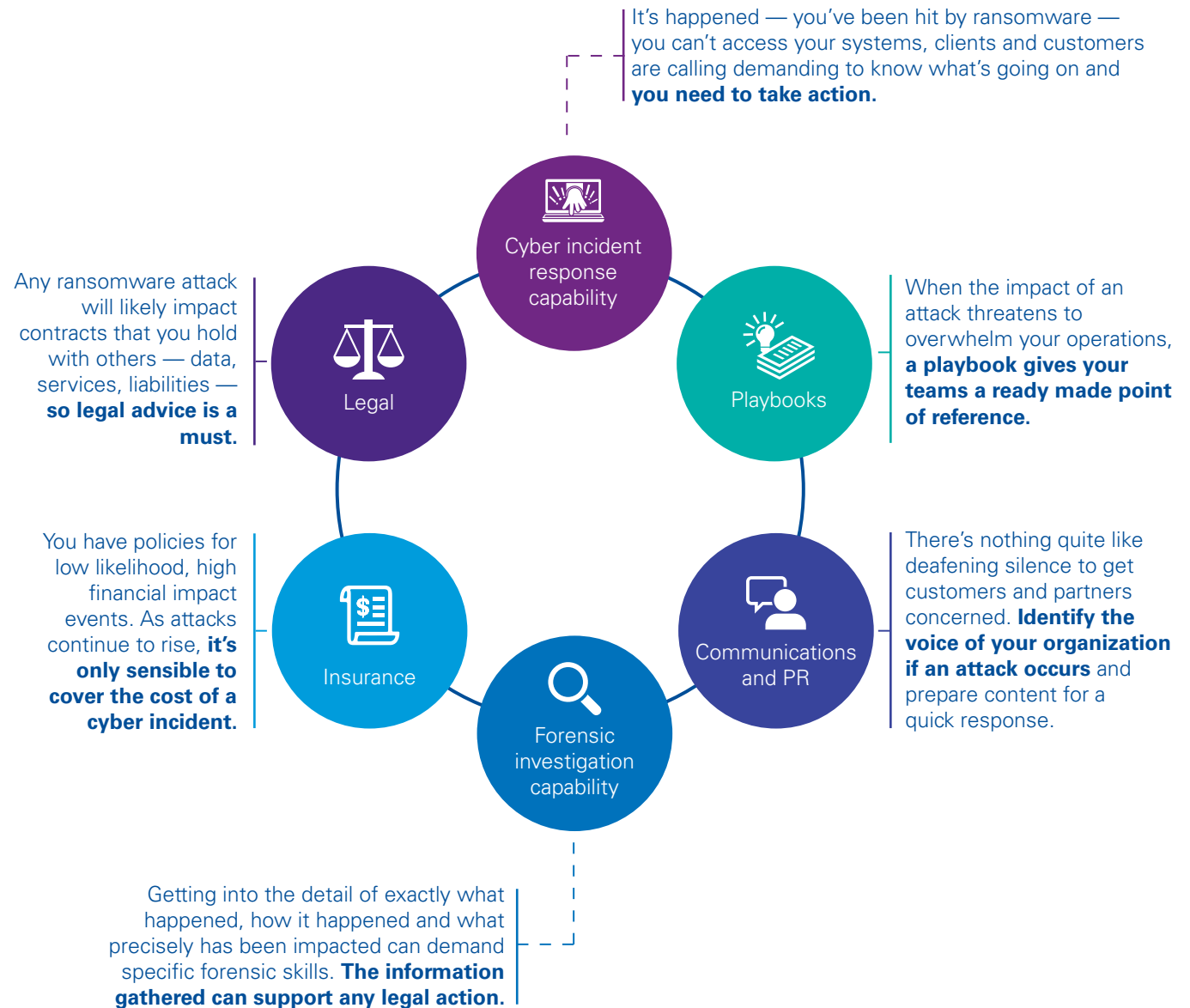


¹⁶ Verizon 2020 Data Breach Investigations Report







Proactive checklists and considerations

 <h3>Assess the basics</h3>	 <h3>Training and awareness</h3>	 <h3>Remote working assessment</h3>	 <h3>Penetration testing</h3>	 <h3>Backups</h3>	 <h3>Incident response exercising</h3>
<p>Checklist:</p> <ul style="list-style-type: none"> — Access – ensure Multi-Factor Authentication (MFA) is applied. <ul style="list-style-type: none"> — Enforce security standards externally (certifications and accreditations). — Audit your IT accounts and privileges regularly – who has access, and do they still need it? — Test for confidence in technical defense. 	<p>Consider:</p> <ul style="list-style-type: none"> — Phishing campaigns – educate end-users on the dangers, what to look out for and how to take action. — eLearning – modules on hacking, data privacy and cyber fraud. — Specialized training— make this specific to business roles and functions, whether the CEO, call center operator or IT administrator, each faces a different challenge. 	<p>Checklist:</p> <ul style="list-style-type: none"> — End-User Device builds – laptop, tablet, smartphone and Endpoint Detection and Response (EDR) Solutions – have you got visibility of these devices and what's happening on them? — Who are the users, what confidential data can they access? Check that they are identified and authenticated when accessing systems. Ensure MFA is applied. — Make sure your IT team can monitor the network, wherever remote working may take it. And that they can filter out anything bad, address vulnerabilities, respond to events and maintain logs of what has happened. 	<p>Test the strength of your defenses and response by getting some 'ethical hackers' to play the role of a cyber criminal.</p> <p>This is known as penetration testing and can be used to:</p> <ul style="list-style-type: none"> — Probe your systems for common vulnerabilities and recommend fixes. — Test your own IT team's response. — Train them in improving defenses and responses to reduce the impact of becoming the victim of a cyber attack. 	<p>If other security controls fail, good backups ensure that you can restore and rebuild, even if your organization suffers an unrecoverable ransomware attack. Be sure to:</p> <ul style="list-style-type: none"> — Test your backups. — Segregate them so that they can't be compromised from a network-wide ransomware incident. — Consider the criticality of your systems — what has the most impact from being 'down' for the longest? What should be restored first? — Consider the data point that you wish to be able to restore from and how quickly. 	<p>Consider the impact on your organization and identify possible courses of action. Think about key systems and services, stakeholders, vendors and suppliers.</p> <p>Consider response metrics, how you might refine processes and critical training requirements and consider how lessons learned may be captured and 'playbooks' developed to speed response.</p>

Responding quickly to an attack — a reactive approach



Reactive checklists and considerations

 <p>Cyber incident response capability</p>	 <p>Playbooks</p>	 <p>Communications and PR</p>	 <p>Forensic investigation capability</p>	 <p>Insurance</p>	 <p>Legal</p>
<p>Effective response capabilities are essential to reduce the impact of a cyber incident. Consider how to:</p> <ul style="list-style-type: none"> — Maintain calm management of the incident, with practical advice on containment, mitigation and restoration of normal business operations. — Get a view of the immediate impact and risks. — Have confidence in your cyber response procedures and controls, and the technologies which underpin them. — Quickly investigate geographically spread networks, people and systems. 	<p>Checklist:</p> <ul style="list-style-type: none"> — Create custom playbooks for each technology to assist with any containment, isolation, recovery and remediation. — Consider a health check as a mechanism of discovering leading practices such as defined and rehearsed actions for ransomware detection and recovery while building or improving playbooks. — Be sure to dig your playbooks out regularly to exercise with and feedback on any possible improvements. 	<p>Think about the impact on your brand and reputation. The importance of good communication to customers, stakeholders, partners and the public can reduce the effects of such incidents.</p> <ul style="list-style-type: none"> — Who will act as the public persona of the organization in such events? — Create pre-prepared content and plans that you can use to speed your response to such events. — Decide if you have the right capabilities in the organization, and if not, consult or engage others and work out how to get their support rapidly if need be. 	<p>There may be a role for forensic investigation in any response. Think about what conditions will demand forensic investigation, including where the triggers and demands of such a view may come from; regulator, customer, law enforcement, the board, insurers, etc.</p> <p>Consider whether you would engage with a third party to fulfill this role and, if so, determine how you would engage with them rapidly and integrate them into your response.</p>	<p>Consider:</p> <ul style="list-style-type: none"> — Immediate costs: largely unavoidable costs that include business and media impact, plus the operational cost of restoring the confidentiality, integrity and availability of data and systems. — ‘Slow-burn’ costs: these vary depending on the incident severity but may include the cost of reimbursing victims/ customers, litigation expenses and regulatory fines and penalties. — Policy requirements: more insurers are demanding a basic level of security as part of the policy. Make sure you satisfy the requirements. 	<p>Legal support becomes key in providing advice and counsel in many facets of a ransomware incident, from views on contractual customer and service provider liabilities to regulatory reporting and determining the legality of some actions in certain geographies, e.g., the paying of ransoms.</p> <p>Does your in-house counsel or retained advisor have this level of specialist knowledge? If needed, how do you engage in getting such expertise?</p>

Staying on top of ransomware

Organizations are accelerating their digital transformation as they look to build functionality and resilience for a post-COVID world. That is likely to see an even greater uptake of cloud services and bring many benefits — and potential risks. Here are some actions you can take now and in the mid-term to improve your cyber security and some challenges your business could face in the future.

Actions to take now

- Assess the impact of system loss on your business and prepare a response action plan.
- Update your security awareness training and resources for post-COVID working.
- Check identity, authentication and access to IT systems.
- Check Endpoint Detection and Response (EDR) capabilities and what you can log and monitor.
- Check your incident response capability and backups.
- Get hacked (by an ethical hacker) and test your response.
- For any future changes, plan security from the start.

Actions for the mid-term

- Consider and check the technology changes you have made for errors.
- Check your remote working setup for vulnerabilities.
- Consider how any business restructure may raise the risk of an 'insider threat.'
- Run an exercise based on a scenario that will have the greatest impact on your organization and learn from it.
- Get hacked (by an ethical hacker) again, and make sure to continually revisit this process as a way of testing your defenses and response.
- Think about what the adoption and expansion of cloud services may mean for shared security responsibility.

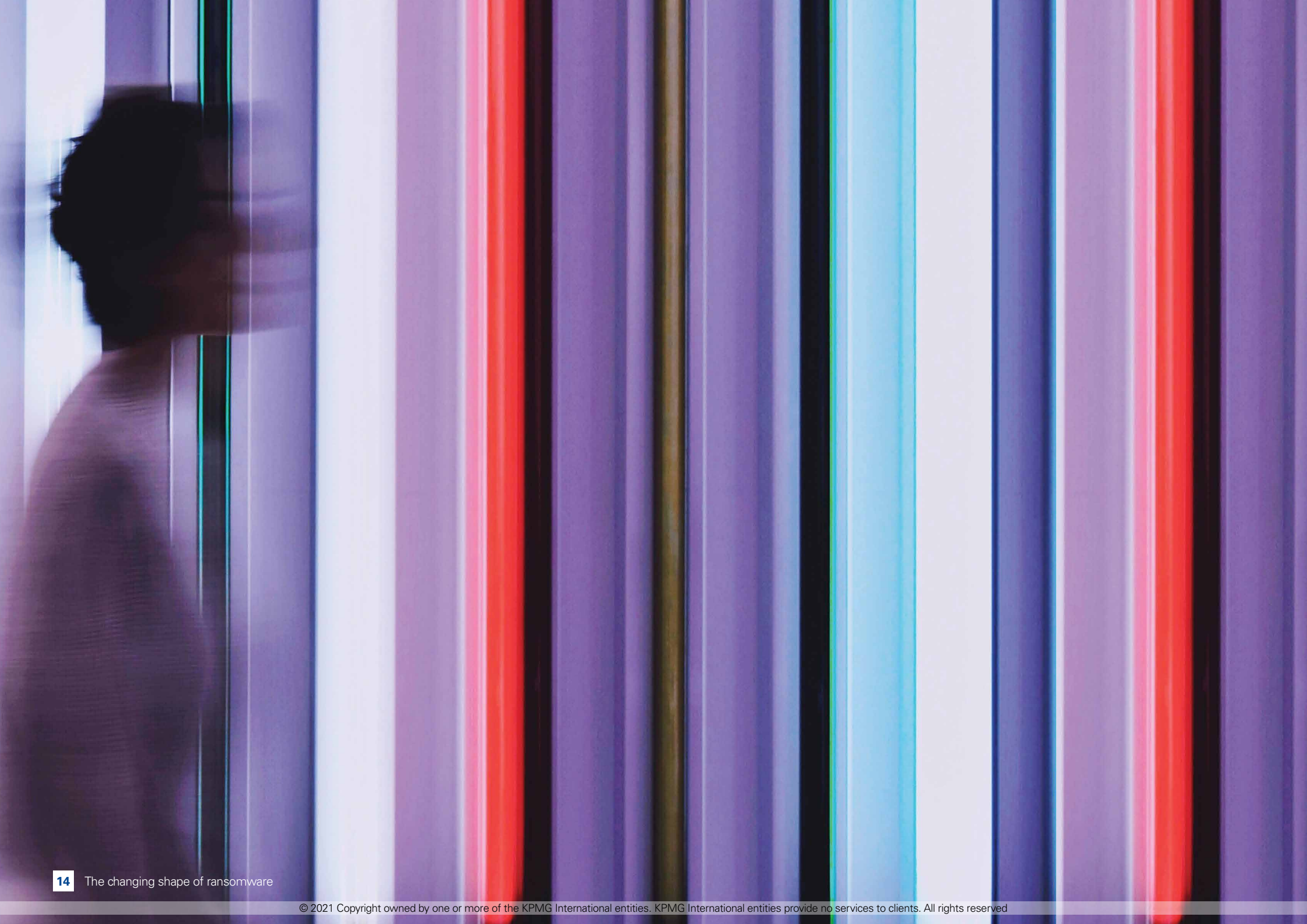
Future trends and challenges

According to KPMG's 2021 CEO Outlook Pulse Survey, the majority of CEOs surveyed point to the amazing progress made in digitizing their operations, business models and revenue streams during the pandemic. Three-quarters (74 percent) say that the speed of digitization has accelerated by a matter of months. In addition, CEOs plan to spend more on digital technologies compared to a year ago, with 49 percent investing heavily in new technologies.¹⁷

With this shift, organizations get out-of-the-box functionality that can be deployed rapidly and managed for them. Yet, adopting new technologies also results in an extended enterprise — adding complexity to information flows and data protection. Questions such as 'Who is responsible for what?' and 'Are risks increased?' must be asked to gain confidence in the extended estate's security.



¹⁷ KPMG CEO Outlook Pulse Survey, 2021



About KPMG

At KPMG, our global organization of cyber security professionals offers a multidisciplinary view of risk. Helping you carry security throughout your organization, so you can anticipate tomorrow, move faster, and get an edge with secure and trusted technology.

No matter where you are on your cyber security journey, KPMG firms have expertise across the continuum — from the boardroom to the data center. In addition to assessing your cyber security and aligning it to your business priorities, we help you develop advanced solutions, implement them, monitor ongoing risks and help you respond effectively to cyber incidents.

KPMG brings an uncommon combination of deep technical expertise, strong business insights and creative professionals who can help you effectively manage and protect your most valuable data across a broad spectrum of evolving threats and scenarios. We approach cyber security, not as a one-time project, but rather a holistic, adaptive strategy aligned to your business goals, focused on delivering long-term value for your business. So you can protect your future and expand possibilities.

Together, let's create a trusted digital world, so we can push the limits of what's possible.

Author



Neil Clarke

Director
Cyber Security Services
KPMG in the UK

Contacts

Edward Goings
**Global Incident Response Lead
and Principal
KPMG in the US**
E: egoings@kpmg.com

Paul Black
KPMG in Australia
E: paulblack1@kpmg.com.au

Gilbert Wondracek
KPMG in Austria
E: gwondracek@kpmg.at

Nico Manavella
KPMG in Argentina
E: nmanavella@kpmg.com.ar

Leandro Antonio
KPMG in Brazil
E: lantonio@kpmg.com.br

Henry Shek
KPMG in China
E: henry.shek@kpmg.com

Juan Marciales
KPMG in Colombia
E: jmarciales@kpmg.com

Timo Piironen
KPMG in Finland
E: timo.piironen@kpmg.fi

Guy Posbic
KPMG in France
E: gposbic@kpmg.fr

Michael Sauermann
KPMG in Germany
E: msauermann@kpmg.com

Manish Tembhurkar
KPMG in India
E: mtembhurkar@kpmg.com

Arhemi Dutimarshelly
KPMG in Indonesia
E: arhemi.dutimarshelly@kpmg.co.id

Dario Amoruso
KPMG in Italy
E: damoruso@kpmg.it

Seosamh Gowran
KPMG in Ireland
E: seosamh.gowran@kpmg.ie

Motoki Sawada
KPMG in Japan
E: motoki.sawada@jp.kpmg.com

Chang-Min Lee
KPMG in Korea
E: changminlee@kr.kpmg.com

Yogesh Beniwal
KPMG in Malaysia
E: ybeniwal@kpmg.com.my

Jefferson Gutierrez
KPMG in Mexico
E: jeffersongutierrez@kpmg.com.mx

Ronald Heil
KPMG in the Netherlands
E: heil.ronald@kpmg.nl

Philip Whitmore
KPMG in New Zealand
E: pwhitmore@kpmg.co.nz

Samuel Asiyabola
KPMG in Nigeria
E: samuel.asiyabola@ng.kpmg.com

Jallain Manrique
KPMG in Philippines
E: jmanrique@kpmg.com

Marcin Strzałek
KPMG in Poland
E: mstrzalek@kpmg.pl

Eddie Toh
KPMG in Singapore
E: eddietoh@kpmg.com.sg

Sergi Gil Lopez
KPMG in Spain
E: sergigil@kpmg.es

Nicolas Tinguely
KPMG in Switzerland
E: ntinguely@kpmg.com

Chanitthikul Nuttanich
KPMG in Thailand
E: nuttanich@kpmg.co.th

Toni Lin
KPMG in Taiwan
E: tonilin@kpmg.com.tw

Oisin Fouere
KPMG in the UK
E: oisin.fouere@kpmg.co.uk

David B. Nides
KPMG in the US
E: dnides@kpmg.com

Phuong Hong Tran
KPMG in Vietnam
E: hptran@kpmg.com.vn

home.kpmg/socialmedia



Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2021 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

KPMG refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity. KPMG International Limited is a private English company limited by guarantee and does not provide services to clients. For more detail about our structure please visit home.kpmg/governance.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

Throughout this document/film/release/website, "we", "KPMG", "us" and "our" refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity.

Designed by Evalueserve.

Publication name: The changing shape of ransomware | Publication number: 137363-G

Publication date: March 2021