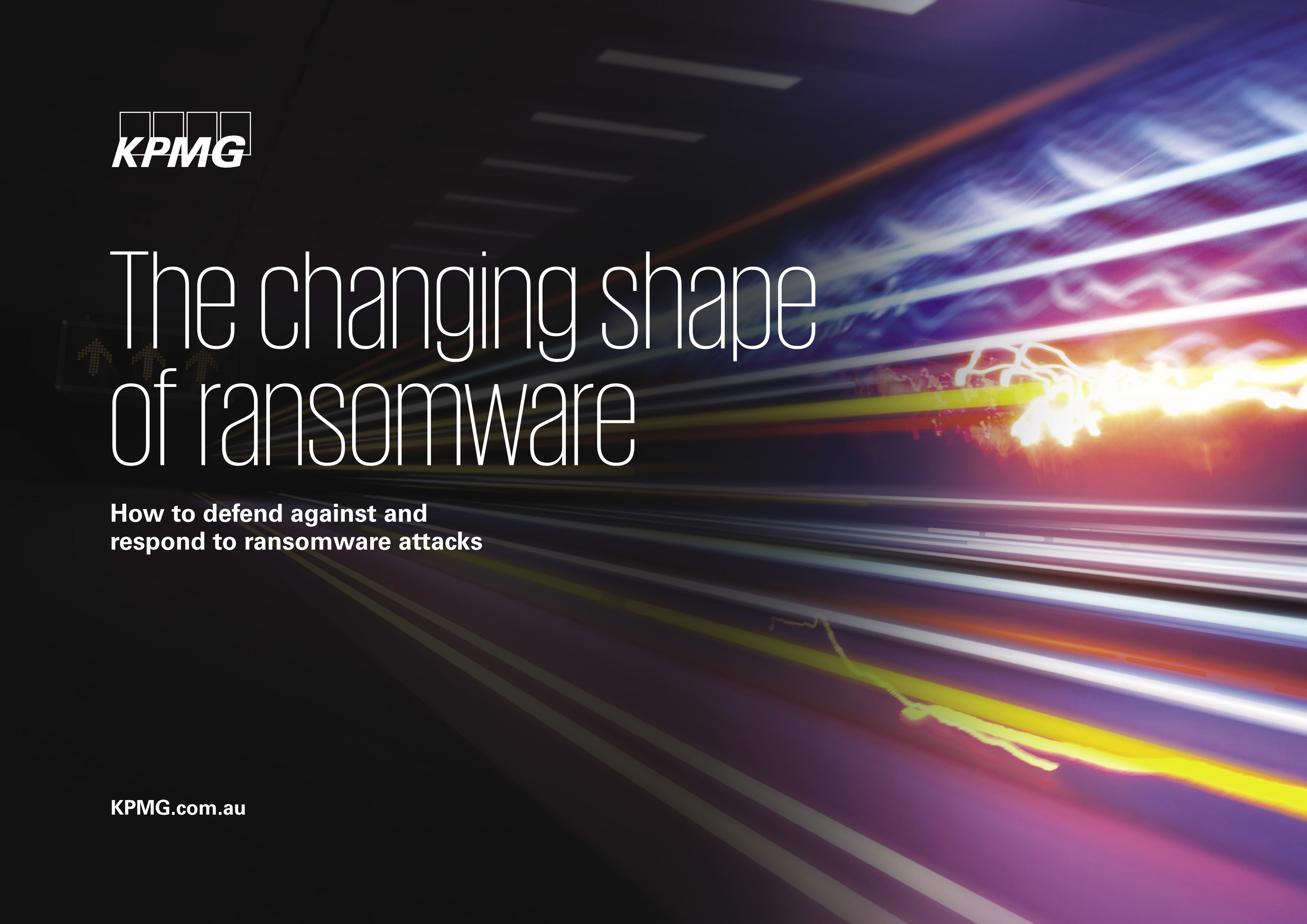


KPMG

The changing shape of ransomware

How to defend against and respond to ransomware attacks

KPMG.com.au

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 capitalised on this disruption. They have further industrialised 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 are seeing an increase in cyber security threats. 41 percent of organisations 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 organisations 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.

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 cyber insurance claims filed in the first half of 2020 were attributed to ransomware[4]

51% of companies said they had a ransomware incident in the last year[5]

100% increase in the average ransom demand from 2019 to Q1 2020[6]

47% further increase in the first 6 months of 2020[7]

[1] Harvey Nash/KPMG CIO Survey, 2020.

[2] KPMG's CEO Outlook Pulse Survey, 2021.

[3] Harvey Nash/KPMG CIO Survey, 2020.

[4] Coalition 2020 Insurance Claims Report, 2020.

[5] Sophos Whitepaper, May 2020.

[6–7] H1 2020 Cyber Insurance Claims Report, Coalition Inc., 2020

Contents

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 organisations 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 may include diversion of staff resources and 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 and a change in their features.[10] Vulnerabilities in people, process and technology controls, due to a move to remote working over this period as well as increased reliance on the Internet of Things, have presented huge opportunities for cyber criminals.

Attackers can use many different methods to get ransomware onto systems, making it difficult to defend against all of these different 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, these risks have increased.

US$1M

The average cost globally to remediate a ransomware attack[11]

21%

of attacks are via emails or phishing[12]

29%

of attacks are via remote access[13]

[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.

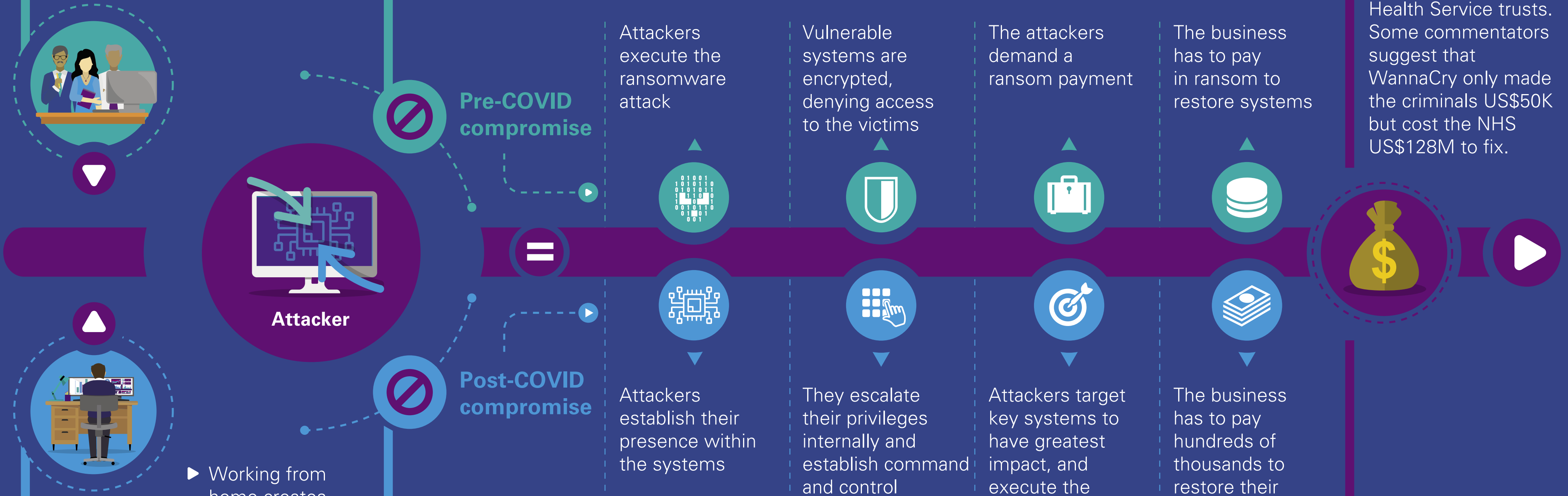
[11] H1 2020 Cyber Insurance Claims Report, Coalition Inc., 2020.

[12–13] Sophos Whitepaper, May 2020.

How attacks have changed as a result of COVID-19

Pre-COVID:
Individuals targeted with a very broad attack path

Two years ago, it was common for cyber criminals to encrypt files, locking out businesses until they paid the ransom. They were broad campaigns, with no specific target, playing the numbers to return revenue, usually in small amounts.



Pre-COVID compromise

- Attackers execute the ransomware attack
- Vulnerable systems are encrypted, denying access to the victims
- The attackers demand a ransom payment
- The business has to pay in ransom to restore systems

Post-COVID compromise

- Attackers establish their presence within the systems
- They escalate their privileges internally and establish command and control
- Attackers target key systems to have greatest impact, and execute the ransomware attack and ransom demand
- The business has to pay hundreds of thousands to restore their systems

▶ Working from home creates 3.5X greater risk[14]

Post-COVID:
Organisations targeted more specifically

Now, hackers often exfiltrate data out as well as encrypting it. They hold the data for ransom and, if no payment is made, data is leaked — which means victims must disclose a data breach to regulators. This could result in a fine (which under GDPR is up to 4% of global revenue).

In May 2017, a WannaCry crypto ransomware affected 80 English National Health Service trusts. Some commentators suggest that WannaCry only made the criminals US$50K but cost the NHS US$128M to fix.

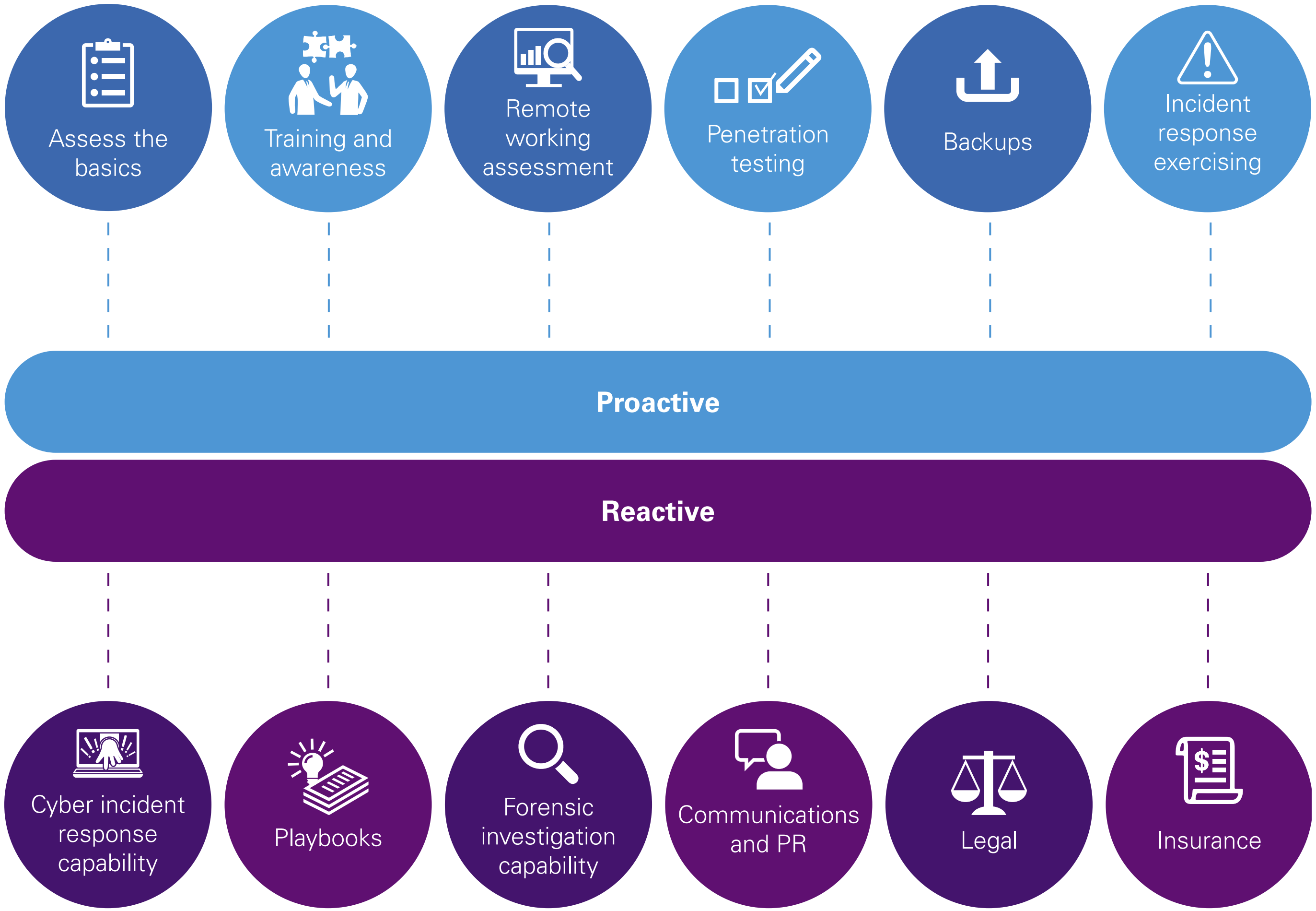
In July 2020, Garmin was hit by a ransomware attack, reported to be the work of Evil Corp, which demanded US$10M to restore systems.

[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.

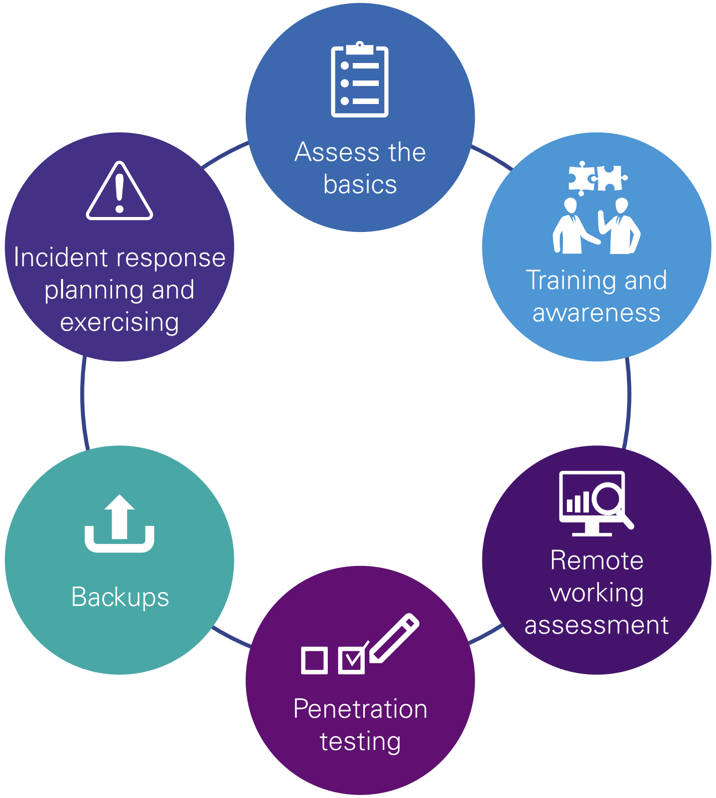
However, if a ransomware attack is successful, reactive steps can be taken to reduce impact and minimise business disruption.



[15] Verizon 2020 Data Breach Investigations Report

Preparing for an attack – a proactive approach

90% of successful cyber attacks are down to a lack of basic controls and defenses against known vulnerabilities; don't be the 'lowest hanging fruit.'[16]


Assess the basics
Incident response planning and exercising
Training and awareness
Backups
Remote working assessment
Penetration testing

Life experience is how we learn. **Simulate the experience so the team can learn from it** and reduce the impact if an attack occurs.

Educate your people on how to protect themselves and the organisation. They are a critical line of defense and an excellent intelligence gathering capability if they know what to look out for.

You'll have to rebuild from scratch if your systems and data are written off following an attack. **Make sure you have backups that you know are safe and work.**

Quickly scaling remote working means IT has enabled many connections rapidly, using new technologies. The risk of setup errors is high. **Take time to check these 'doors in'**; it only takes a few days.

'Train hard, fight easy,' try hacking your organisation like a cyber criminal would; **identify issues and fix the basics in a week.**

[16] Verizon 2020 Data Breach Investigations Report

Proactive checklists and considerations

Assess the basics

- Access – ensure Multi-Factor Authentication (MFA) is applied.
  - Enforce security standards externally (certifications and accreditations).
  - Robust credential tracking.
  - Audit your IT accounts and privileges regularly – who has access, and do they still need it?
- Test for confidence in technical defence.

Training and awareness

- 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.
- Specialised training– make this specific to business roles and functions, whether the CEO, call centre operator or IT administrator, each faces a different challenge.
- Test your response teams through simulated scenarios and exercises.
- Track security metrics. In what ways is your organisation being targeted and where are the near-misses happening? Learn and adapt based on this data.

Remote working assessment

- 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.

Penetration testing

- Test the strength of your defences and response by getting some 'ethical hackers' to play the role of a cyber criminal. This is known as penetration testing and can be used to:
  - Probe your systems for common vulnerabilities and recommend fixes.
  - Test your own IT team's response.
  - Train them in improving defences and responses to reduce the impact of becoming the victim of a cyber attack.

Backups

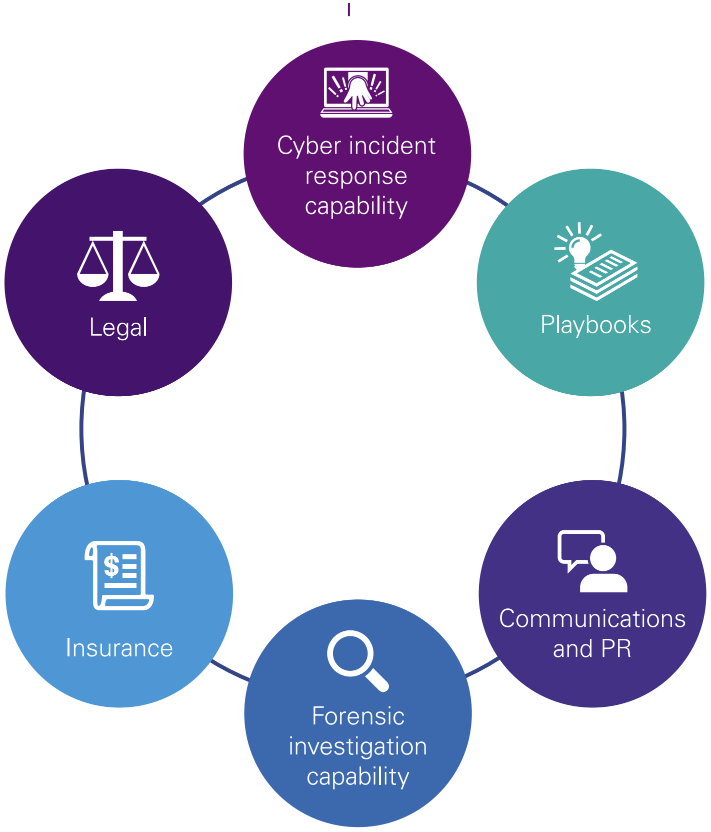
If other security controls fail, good backups ensure that you can restore and rebuild, even if your organisation suffers an unrecoverable ransomware attack. Be sure to:

- 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.

Incident response exercising

- Your key cyber risks and their likely impact on the organisation.
- Your critical data including IP, commercially sensitive and personal data.
- Required support when a cyber attack occurs. Engage and involve expert advisors in your response planning processes.
- Mitigation strategies and possible courses of action.
- Impacts on key systems and services, data, stakeholders, vendors and suppliers.
- Your cyber insurance cover and response requirements.
- Potential legal and regulatory exposure and notification obligations.

Responding quickly to an attack — a reactive approach


Cyber incident response capability
Playbooks
Communications and PR
Forensic investigation capability
Insurance
Legal

It's happened — you've been hit by ransomware — you can't access your systems, clients and customers are calling demanding to know what's going on and **you need to take action.**

When the impact of an attack threatens to overwhelm your operations, **a playbook gives your teams a ready made point of reference.**

There's nothing quite like deafening silence to get customers and partners concerned. **Identify the voice of your organisation if an attack occurs** and prepare content for a quick response and regular updates.

Getting into the detail of exactly what happened, how it happened and what precisely has been impacted as well as preserving evidence and data can demand specific forensic skills. **The information gathered can support or help defend any legal action.**

You have policies for low likelihood, high financial impact events. As attacks continue to rise, **it's only sensible to cover the cost of a cyber incident.**

Any ransomware attack will likely impact contracts that you hold with others — data, services, liabilities — **so legal advice is a must.**

Reactive checklists and considerations

Cyber incident response capability

Effective response capabilities are essential to reduce the impact of a cyber incident. Consider how to:

- 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 networks, people, data and systems.

Playbooks

- 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.

Communications and PR

Think about the impact on your brand and reputation. The importance of good communication to customers, staff, stakeholders, partners and the public can reduce the effects of such incidents.

- Who will act as the public persona of the organisation 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 organisation, and if not, consult or engage others and work out how to get their support rapidly if need be.

Forensic investigation capability

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.

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. Ideally they should be onboarded and retained before any incident and ready to respond.

Insurance

- Consider immediate 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, ongoing legal and forensic advice, 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.

Legal

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 drafting notices, liaising with relevant agencies, ensuring communications and reports are privileged and determining the legality of some actions in certain geographies, e.g., the paying of ransoms.

- Does your in-house counsel or retained advisor have this level of specialist knowledge? If needed, how do you engage in getting such expertise? Again, ideally they should be onboarded and retained before any incident.

Staying on top of ransomware

Organisations 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, cyber risk management and and cyber resilience and some challenges your business could face in the future.

Actions to take now

— Assess the potential impacts of system and data loss on your business and prepare a response action plan. Consider how your organisation would respond to a ransom demand and test this

— 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 organisation 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 digitising their operations, business models and revenue streams during the pandemic. Three-quarters (74 percent) say that the speed of digitisation 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, organisations 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 organisation's cyber resilience. What are the potential impacts on individuals, customers and the organisation if these are compromised?'

[17] KPMG CEO Outlook Pulse Survey, 2021

About KPMG

At KPMG, our cyber security forensic and legal professionals offer a multidisciplinary view of risk and incident response. Helping you embed security throughout your organisation, so you can anticipate tomorrow, become more cyber resilient, identify and manage your cyber risks, move faster, and get an edge with secure and trusted technology.

No matter where you are on your cyber security and resilience journey, KPMG has expertise across the continuum — from the boardroom to the data centre. In addition to assessing your cyber security risk and resilience and aligning these 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 and multidisciplinary expertise, strong business insights and creative professionals who can help you effectively manage and protect your systems, networks and most valuable data across a broad spectrum of evolving threats and scenarios. We approach cyber security and resilience, 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.

Contacts

Paul Black
Partner
Forensic and National Lead,
Cyber Incident Response
T: +61 2 9458 1583
E: paulblack1@kpmg.com.au

Kate Marshall
Head of KPMG Law
T: +61 3 9288 5767
E: katemarshall@kpmg.com.au

Gordon Archibald
National Lead
Cyber Security Services
T: +61 2 9346 5530
E: garchibald@kpmg.com.au

Veronica Scott
Privacy, Digital & Data Protection Lead
KPMG Law
T: +61 3 8667 5711
E: vscott1@kpmg.com.au

KPMG.com.au

The information contained in this document is of a general nature and is not intended to address the objectives, financial situation or needs of any particular individual or entity. It is provided for information purposes only and does not constitute, nor should it be regarded in any manner whatsoever, as advice and is not intended to influence a person in making a decision, including, if applicable, in relation to any financial product or an interest in a financial product. Although we endeavour 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.

To the extent permissible by law, KPMG and its associated entities shall not be liable for any errors, omissions, defects or misrepresentations in the information or for any loss or damage suffered by persons who use or rely on such information (including for reasons of negligence, negligent misstatement or otherwise).

Liability limited by a scheme approved under Professional Standards Legislation.

April 2021. 672683606MC