The changing shape of ransomware

How to defend against and respond to ransomware attacks

KPMG International

www.kpmg.ch/cyber

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

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 accounts[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.
[3–4] Harvey Nash/KPMG CIO Survey, 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 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.

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.

Post-COVID:
Organizations targeted more specifically

Working from home creates 3.5X greater risk[14]

Pre-COVID compromise

Post-COVID compromise

Attacker

Attackers execute the ransomware attack

Attackers establish their presence within the systems

Vulnerable systems are encrypted, denying access to the victims

They escalate their privileges internally and establish command and control

The attackers demand a ransom payment

Attackers target key systems to have greatest impact, and execute the ransomware attack and ransom demand

The business has to pay thousands in ransom to restore systems

The business has to pay hundreds of thousands to restore their systems

In May 2017, a WannaCry 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.

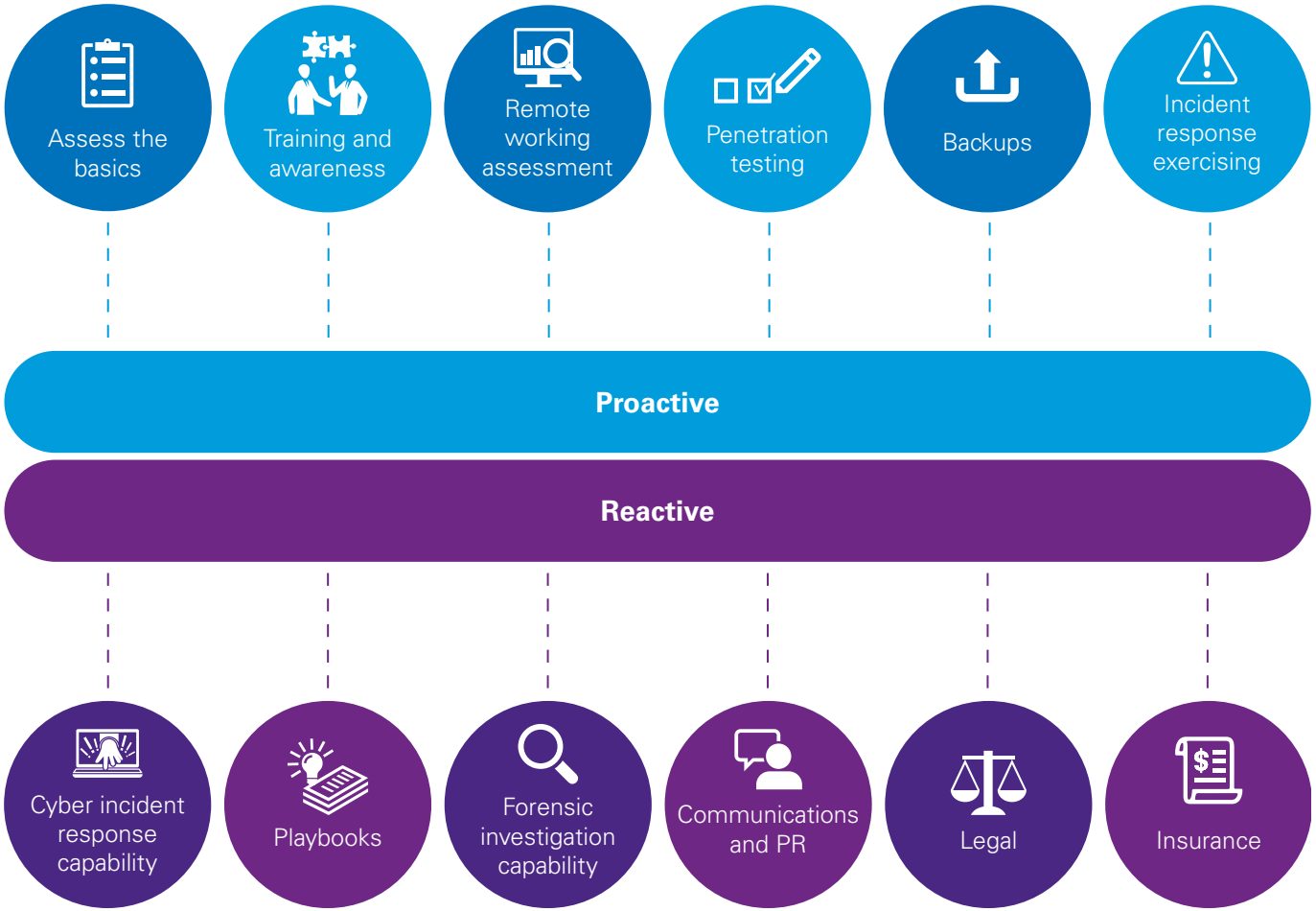
Now, hackers often smuggle data out as well as encrypting it. They hold the data for ransom and, if no payment is made, data is leaked — forcing victims to disclose a data breach to regulators. This admission could result in a fine (up to 4% of global turnover).

[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

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]

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 organization. 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 organization 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

Checklist:

- Access – ensure Multi-Factor Authentication (MFA) is applied.
  - 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.

Training and awareness

Consider:

- 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.

Remote working assessment

Checklist:

- 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 defenses 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 defenses 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 organization 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

Consider the impact on your organization and identify possible courses of action. Think about key systems and services, stakeholders, vendors and suppliers.

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.

Responding quickly to an attack — a reactive approach

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 geographically spread networks, people and systems.

Playbooks

Checklist:

- 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, stakeholders, partners and the public can reduce the effects of such incidents.

- 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.

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.

Insurance

Consider:

- 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.

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 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?

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

Your contacts in Switzerland

KPMG AG
Räffelstrasse 28
PO Box
8036 Zurich

Dr. Matthias Bossardt
Partner
Head of Cyber Security Consulting

+41 58 249 36 98
mbossardt@kpmg.com

Dr. Thomas Bolliger
Partner
Cyber

+41 58 249 28 13
tbolliger@kpmg.com

Nicolas Tinguely
Director
Cyber

+41 58 249 21 44
ntinguely@kpmg.com

Yves Bohren
Director
Cyber

+41 58 249 48 95
ybohren@kpmg.com

kpmg.ch/cyber