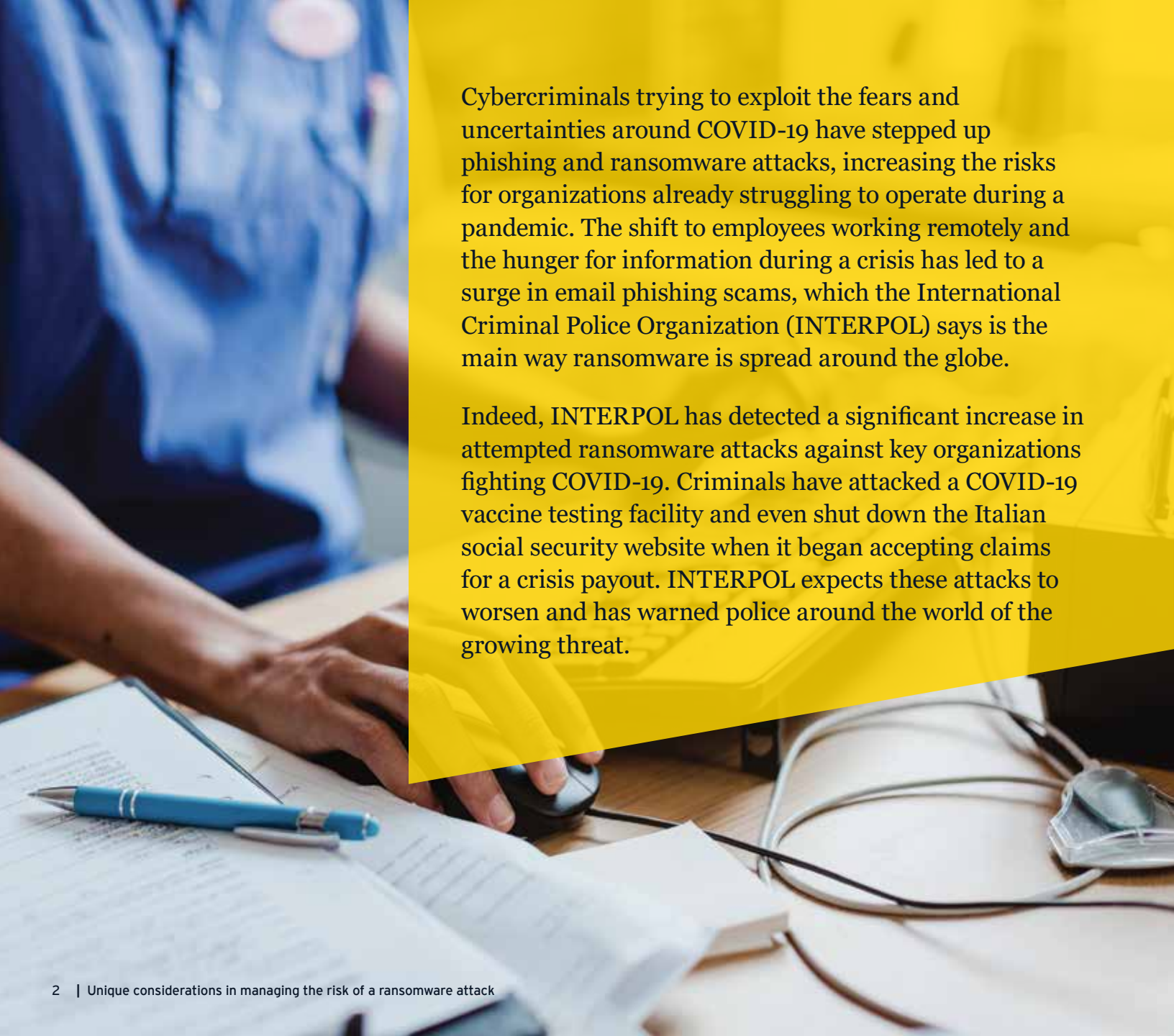
Unique considerations in managing the risk of a ransomware attack

Legal, Compliance and Technology Executive Series

EY
Building a better working world



Cybercriminals trying to exploit the fears and uncertainties around COVID-19 have stepped up phishing and ransomware attacks, increasing the risks for organizations already struggling to operate during a pandemic. The shift to employees working remotely and the hunger for information during a crisis has led to a surge in email phishing scams, which the International Criminal Police Organization (INTERPOL) says is the main way ransomware is spread around the globe.

Indeed, INTERPOL has detected a significant increase in attempted ransomware attacks against key organizations fighting COVID-19. Criminals have attacked a COVID-19 vaccine testing facility and even shut down the Italian social security website when it began accepting claims for a crisis payout. INTERPOL expects these attacks to worsen and has warned police around the world of the growing threat.

Defending against ransomware attacks

Of special interest to:
Legal counsel
Corporate security officers
Information security executives
Compliance executives
Risk management executives
Internal audit

All it takes is for one person to click on a link in a fraudulent email to cause malware spreading through an organization's network in a matter of minutes and encrypting critical data. Before long, the organization is unable to access its vital files and systems until it pays off the criminals to obtain a decryption key or finds other ways to recover its data.

Building employee awareness is critical

Despite the increasing attacks, there are many measures organizations can take to reduce the success rate of attack attempts. Educating employees on the growing threat of ransomware and the organization's security protocols is the first line of defense. A global 2020 survey found less than one-third of working adults could explain the term ransomware. In fact, nearly 30% of US employees said malware is a type of hardware that boosts Wi-Fi signals, rather than software designed to damage or gain unauthorized access to a computer system.[1]

Employees should be given guidance on how to detect suspicious emails and promptly bring them to the organization's attention. Researchers who sent simulated phishing emails to health care organizations found nearly 17% of employees clicked on what could have been a malicious link. But as more simulated threats were sent and employee education followed, click rates were significantly reduced.[2]

Education should also cover a broad range of scenarios for how ransomware can be spread. It's important that remote workers understand that lack of precaution can enable attackers to use tools like remote desktop protocol to penetrate an organization's network, and perpetrate a ransomware attack. A user can unknowingly visit an infected website where malware is downloaded or fall prey to a malware disguised as legitimate software.

1 *2020 State of the Phish Annual Report*, Proofpoint, 2020, https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-state-of-the-phish-2020.pdf.

2 William J. Gordon, Adam Wright, and Ranjit Alyagari, "Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions," *Journal of the American Medical Association*, 8 March 2019, https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2727270.

Organizations must marshal an array of defenses

Backing up data is critical to defending against ransomware, but many organizations store backup data on the same network they regularly use. This allows an attacker to encrypt backup data just as easily as files on a company's regular operating system. To keep backups safe, they must either be placed in a segregated network or placed offline. For example, following a spate of attacks against hospitals, many now regularly put backups of critical systems offline. This allows a hospital to access essential data if the main network is shut down. However, even if an organization protects its backup data, it can take days or even weeks to restore systems.

Good cybersecurity hygiene also includes patch management, hardened configurations and ongoing detection enabled by threat intelligence. It's also important to apply software updates for browsers and plug-ins as soon as they are released. Encrypting sensitive information is another way to defend against cybercriminals who threaten to release information publicly if a ransom isn't paid.

Organizations should also engage neutral third parties to conduct regular audits of their preventative measures for ransomware and other cyber breaches. Cybersecurity insurance is becoming increasingly common, but it is not a substitute for good security — insurers can refuse to pay claims if organizations fail to use or disclose their lack of appropriate security procedures.

Responding to a ransomware attack

As the risk of cyber attacks continues to rise, many organizations are putting more emphasis on quick detection and containment. Every organization should have an incident response and recovery plan that is regularly assessed and refreshed. Be sure to include all appropriate stakeholders, such as IT, information security, legal, compliance, human resources, operations and communications. Response plans should clearly define responsibilities and enable stakeholders to lead effectively in crisis.

Legal counsel should be engaged the moment an attack is discovered. Counsel can advise on conducting the investigation in a manner that will stand up to scrutiny in the organization's operating jurisdiction(s) and staying compliant with the relevant notification requirements of data protection and privacy regulations. Retaining outside counsel allows an organization to maintain privilege if the breach leads to litigation.

Unique considerations in a ransomware attack response

Responding to a cyber breach usually includes four parallel activities: investigation, containment, eradication and recovery. These activities are generally the same regardless of the type of attack. However, there are unique considerations when dealing with ransomware.

Evidence collection for investigation needs to focus on how the attackers entered the environment, how malware was utilized, the potential path the attackers traveled and what data was taken or encrypted, if any. Bitcoin wallets provided in the ransom note and communications with the attackers need to be carefully documented as they are important for containment, eradication and recovery stages.

Victimized organizations should conduct investigations beyond the systems affected by the attack. Frequently, other malware or dormant ransomware is found hidden in the environment that has not appeared impacted. Making sure that all vestiges of malware hidden in a network are eliminated is critical to avoid the recurrence of the incident.

Regulatory notification expectations

Some jurisdictions define ransomware infections as a cyber breach triggering regulatory and statutory notification requirements. Knowing which geographies are impacted will help organizations enact the appropriate procedures. US health care providers regulated by the Health Insurance Portability and Accountability Act (HIPAA) are obligated to report a ransomware attack as a security incident. HIPAA also requires covered organizations to implement security measures to help prevent ransomware, such as backing up data.

Organizations also need to understand if personally identifiable information (PII) is affected and if so, how it is affected, and consult with their legal counsel on whether it should be considered loss of data and subject to notification requirements by relevant data protection and privacy regulations or laws (e.g., EU's General Data Protection Regulation, The California Consumer Privacy Act).

Legal and regulatory concerns about paying ransom

Unlike other cyber breaches, there is typically one simple way to stop the attack and decrypt files — pay the ransom demanded. Besides the obvious ethical dilemma, the decision to pay off a criminal has many legal implications.

Throughout the world, law enforcement advises against paying ransom. The US Federal Bureau of Investigation shares decryption keys for some types of common malware. The No More Ransom website, which is supported by European police agencies, also shares decryption keys and offers ways to report attacks to law enforcement agencies around the world. A 2020 Proofpoint survey found that 29% of organizations never gained access to their data after paying ransom — some even paid more than once, for reasons unspecified by the survey.[3]

New York State is considering two bills that would make it illegal to pay ransom in a cyber attack. A ransom payment could violate US sanctions against terrorism if the attacker is found to be part of a known terrorist group.

Businesses should also be aware that hiring an outside service to recover data after an attack could result in a ransom being paid without their knowledge. A ProPublica investigation found two US firms that offered to unlock victims' data with their own recovery methods actually paid ransom money to secure decryption tools.[4] If the organization engages an external resource to aid in recovery, it should be vetted carefully and explicitly asked whether a ransom will be paid.

[3] *2020 State of the Phish Annual Report*, Proofpoint, 2020, https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-state-of-the-phish-2020.pdf.

[4] Renee Dudley and Jeff Kao, "The Trade Secret — Firms That Promised High-Tech Ransomware Solutions Almost Always Just Pay the Hacker," *ProPublica*, 15 May 2020, https://features.propublica.org/ransomware/ransomware-attack-data-recovery-firms-paying-hackers/.

In summary

The COVID-19 crisis is increasing the risks from ransomware attacks, especially for organizations with limited resources. But risk can be mitigated both through preventative measures, and by moving quickly to detect and contain successful breaches. While many employees view cybersecurity as an IT issue, educating users on how to recognize and flag ransomware is a critical part of any defense. Organizations must develop a sound back-up plan so they can recover lost data quickly and reduce operation downtime and lost productivity.

But prevention alone isn't the answer. An organization's ability to quickly detect, contain and recover from ransomware attacks will impact its continuity of operations and economic losses. In addition, an effective response strategy will ultimately enhance an organization's ability to detect and respond to future attacks. Organizations that decide to pay ransom to decrypt their data must ensure malware doesn't remain hidden in their systems.

Legal and compliance professionals can aid their organizations by understanding the potential regulatory and legal issues resulting from a ransomware attack. IT professionals aren't the only ones who need to develop an effective response strategy for these often-crippling attacks — every stakeholder with a role to play in mitigating risk should do the same.

For more information,
contact EY Cyber Response Services at:

CyberResponse@ey.com
or visit us at:
ey.com/CyberResponse

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

About EY Forensic & Integrity Services
Embedding integrity into an organization's strategic vision and day-to-day operations is critical when managing complex issues of fraud, regulatory compliance, investigations and business disputes. Our international team of more than 4,000 forensic and technology professionals helps leaders balance business objectives and risks, build data-centric ethics and compliance programs, and ultimately develop a culture of integrity. We consider your distinct circumstances and needs to assemble the right multidisciplinary and culturally aligned team for you and your legal advisors. We strive to bring you the benefits of our leading technology, deep subject-matter knowledge and broad global sector experience.

© 2020 EYGM Limited.
All Rights Reserved.

EYG no. 002427-20Gbl
WR #2004-3466945
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com

Contacts:

Arpinder Singh
Partner and Head – India and Emerging Markets
Forensic & Integrity Services, EY
arpinder.singh@in.ey.com
+ 91 12 4443 0330

Harshavardhan Godugula
Partner and Forensic Technology Lead
Forensic & Integrity Services, EY
harshavardhan.g@in.ey.com
+ 91 40 6736 2234

Ranjeeth Bellary
Associate Partner
Forensic & Integrity Services, EY
ranjeeth.bellary@in.ey.com
+ 91 22 6192 0172