Sponsored by EY Forensic & Integrity Services

Important considerations for responding to ransomware attacks

Of special interest to:

General counsel

Outside counsel

Chief legal officer

Legal technology executives

Chief compliance officer

Legal, Compliance and Technology Executive Series

The "WannaCry" malware has brought the topic of ransomware back to front and center in the news. The spread of the initial malware variant may seem to have abated, but many security researchers anticipate that a new variation will likely appear in the near future.

Ransomware has to get through the first locked door of the IT environment before it can start moving around the network. That first step usually happens when someone clicks on a link, browses an infected site or opens an attachment with malicious content embedded.

Good cybersecurity hygiene enforced by ongoing detection is critical to prevent major outbreaks from ransomware or any other type of malware. Organizations should adopt restrictive policies around email attachments, websites and content that can be viewed on the internet. Equally important are awareness programs that educate employees on the perils of malware and on the security control measures to protect critical digital assets. Finally, a company should consider establishing or strengthening its security operations center that is powered by real-time threat intelligence and endpoint security technologies leveraging machine learning and other advanced analytics.

The risk of being attacked increases exponentially when preventative measures are not taken, but any wall can be breached. Failure to take cyber breach response equally seriously can mean the difference between hours and days versus weeks and months of system compromise and outage.

EY

Building a better working world

Key considerations when responding to a ransomware attack

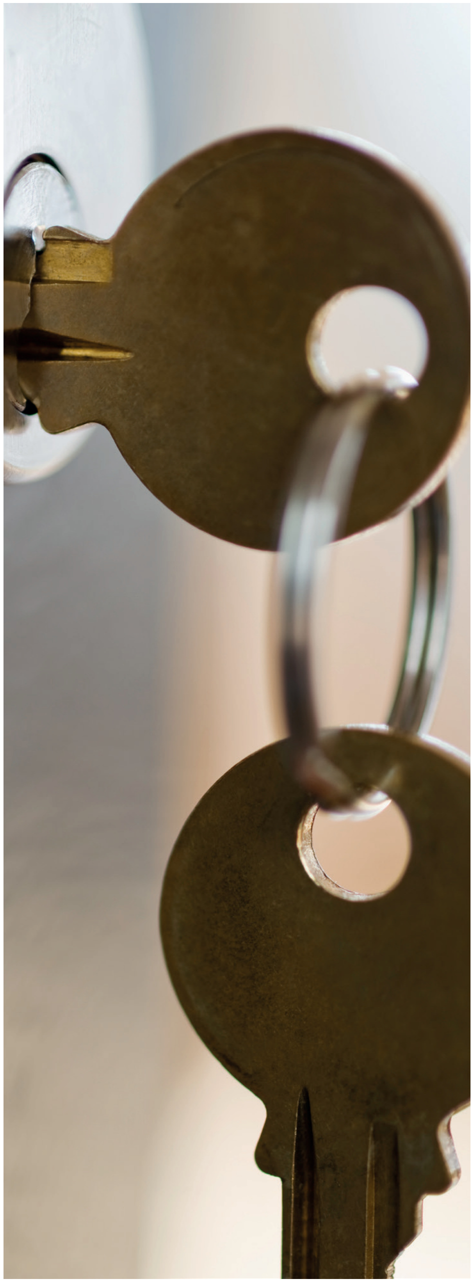
Do not treat the response as just an IT problem. Every organization should have a cyber breach response plan that's regularly refreshed and validated using tabletop exercises. The plan needs to involve stakeholders from the relevant functional areas (e.g., legal, compliance, information security, PR, HR). It should include a communications channel that doesn't depend on IT systems (which could be infected). The stakeholers involved need a constant stream of up-to-date information in order to lead effectively in crisis as well as coordinate with each other in real time and make prudent decisions.

Input from legal is vital, and oftentimes companies retain outside counsel to direct these investigations in anticipation of notification procedures, litigation and regulatory inquiries. Companies should always involve counsel when interacting with law enforcement. Legal helps conduct the investigation in a manner that will stand scrutiny in its operating jurisdiction(s). They can also help companies understand the legal risks from accessing or exposing potentially sensitive information (e.g., customer, third-party partner, employee) during investigations.

There are four parallel imperatives when responding to a ransomware attack: investigation, remediation, eradication and recovery. We will focus the rest of this paper on activities in support of investigation.

Common misperceptions about ransomware attacks

Misperception	Truth
"Everyone gets hit by ransomware. It's is no big deal as long as you get the hackers to unlock the data."	▸ Most large breaches are the product of smaller, unresolved incidents. ▸ Significant breaches almost never appear to be significant on day one.
"Our technical teams decrypted the data, so case closed."	▸ Ransomware can act as an anti-forensic tool rather than an end unto itself, which means that it's designed to fool you. ▸ Hackers frequently leave behind malware that allows them to remain in your system. ▸ Depending on the jurisdiction(s) you operate in, the fact that some types of data were accessed by the ransomware may trigger regulatory inquiries or statutory requirements.
"This only impacted a handful of machines."	▸ Depending on how the ransomware was deployed, it may be a symptom of a larger compromise.



Activities for investigation

Containment

Ransomware attacks seek to encrypt as many systems as fast as possible. Essentially, encryption is like scrambling the tumblers on a safe so that the combination to access valuables no longer works. To limit the number of systems the hackers can scramble, it is important to disconnect and power down infected machines as rapidly as possible. Companies also should take their backup systems offline to prevent them from becoming encrypted. Consider blocking all zip files from being transmitted over email, as this is one of the primary avenues through which this type of attack can propagate.

Collection and preservation of evidence

Facts matter, both for remediation of the breach and for dealing with the legal and regulatory actions that will follow. Evidence collection must be performed in a forensically sound manner so that it can be credibly presented in court or to a regulatory body.

Digital forensics seeks to preserve evidence in its original form, in a bit-for-bit format, mirroring the original data. Make multiple copies of the preserved data to minimize further chance of data loss and maximize the opportunity for a full recovery. The preserved information and system copies can provide an "investigation baseline" that the company can use when analyzing the impact and scope of the breach. Further, the company can enable the investigators to work in a "sandbox" without running the risk of the original data being destroyed.

Infected IT systems must be treated as a crime scene. First responders should capture as much information as possible such as:

- Emails and bitcoin addresses provided by the hackers
- The ransom note
- The locations of every device that appears to be infected
- The contact information of all witnesses to the event
- Network logs
- Who conducted what activity and when that led to the discovery of the attack

Centralize the documents obtained and retain them in an offline backup in order to preserve their integrity. For certain situations, it may be necessary to restore the original data to a completely new environment.

Forensic analysis and impact assessment

To avoid conflict of interest, the investigation team should not be the team responsible for cybersecurity prevention. It is important that the investigation team conduct a comprehensive forensic examination to determine the attack vector, the scope and depth of the compromise. Leave no stones unturned. For example, the ransom note usually contains a bitcoin wallet number that can be used to trace the source of the bitcoin wallet. The information about the source can help investigators uncover additional evidence or the perpetrators themselves. Investigators can follow an attacker's lateral movement through an enterprise by using the attacker's exploitation techniques, tools and procedures.

Forensic analysis is critical to understand the scope of compromised systems and the extent of data exfiltration. Companies need to understand what sensitive data (e.g., customer or employee PII, trade secret) is impacted to determine the risk impact. They can then assess the legal and compliance risks in order to determine appropriate response activities in a timely manner. Some jurisdictions define ransomware infections as a cyber breach triggering regulatory and statutory notification requirements. Knowing which geographies are impacted will help companies enact the appropriate notification procedures.

In short, a forensics investigation team should be able to answer important questions such as:

- When did the attacker/malware get inside?
- What did the attacker do when they got inside?
- What critical information did the attacker access?
- What did the attacker take?

The forensics investigation team usually have access to a repository of keys and applications that can decrypt data locked by different types of ransomware. In some cases, forensic investigators may be able to decrypt files and recover them in their entirety, or recover partial information. If a company decides to pay the ransom, it is also important to engage the forensics team in setting up the bitcoin wallet to avoid fraud.

Reporting and documentation

Companies need to work with their investigators to create detailed documentation of all response activities, including the dates and times of the tasks and person(s) who performed the tasks. A lot of things can be happening at once during a crisis. Without sufficient documentation, it can be difficult to reconstruct the information needed during remediation efforts, post-incident legal proceedings or regulatory inquiries.

Engaging legal and compliance early in an investigation can also help companies be better prepared in obtaining the right data needed for varying requirements, whether they are for regulatory reporting, disputes, litigation, notification or insurance claim. For global companies, cross-border collaboration is also critical to take into account local laws and regulations.

In summary

How companies respond to ransomware attacks matters. A company's response will impact the continuity of operations, as well as its ability to respond to potential regulatory inquiries and legal actions. Here are the key steps to take in the event of a ransomware attack:

- Disconnect infected machines from the network and take all backups offline
- Activate the business continuity plan to minimize disruption to the business and prepare for quick recovery
- Collect and preserve evidence in a forensically sound manner
- Activate the incident response plan and engage cross-functional stakeholders in the investigation
- Prepare data and documentation in anticipation of regulatory reporting, insurance claim and dispute, litigation and customer notification

Successful execution of these actions will help a company prepare for remediation, eradication and recovery activities. In addition, an effective response strategy will ultimately enhance its ability to detect and respond to future attacks.

For more information, contact EY Cyber Response Services at:

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

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. For more information about our organization, please visit ey.com.

About EY Forensic & Integrity Services
Dealing with complex issues of fraud, regulatory compliance and business disputes can detract from efforts to succeed. Better management of fraud risk and compliance exposure is a critical business priority — no matter the size or industry sector. With approximately 4,500 forensic professionals around the world, we will assemble the right multidisciplinary and culturally aligned team to work with you and your legal advisors. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide.

EYG No. 03341-171Gbl
BSC No. 1807-2805276

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.

Any reference to legal rulings and interpretations of their impact is not legal advice. You should consult your legal advisor for guidance on how the cited cases may be applicable to or impact your situation based on the facts of any particular matter.

ey.com