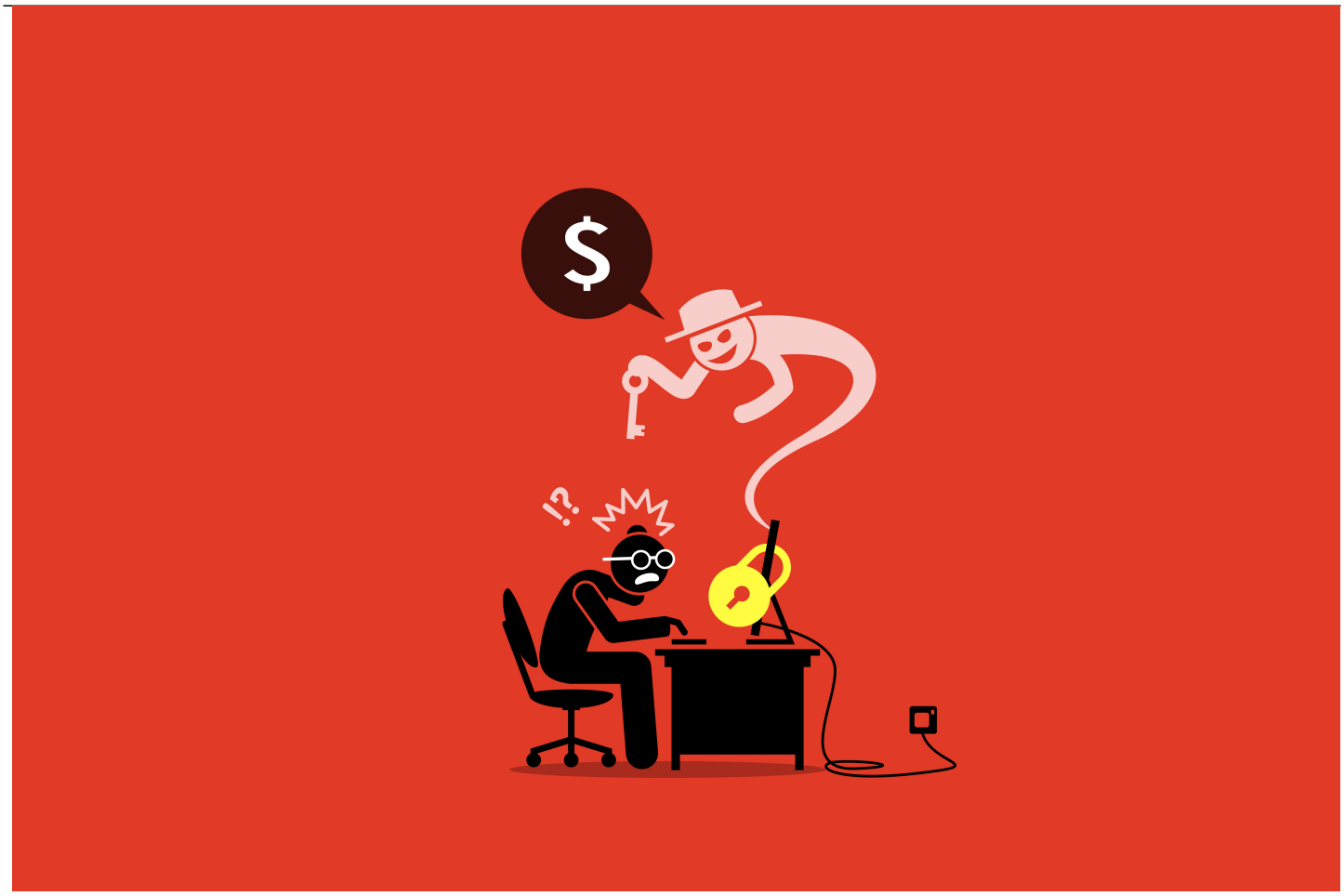
ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

# Don't Let Your Company’s Reputation be Held for Ran$om

**Technology, Privacy, and eCommerce**



Banner artwork by Leremy / *Shutterstock.com*

Did you know that ransomware operators take customer service very seriously, even going so far as to have call centers to ensure customer satisfaction and prompt service? And what is their currency-in-trade? Your organization's reputation, confidential data, and your personal information! They certainly take their business of data theft and extortion, and of collecting your payment via cryptocurrency, very seriously indeed. This poses serious risks to the confidentiality, privacy, and compliance of your organization. Guarding against a ransomware attack through robust security tools and processes is key to not becoming the next victim.

## What is ransomware?

Traditionally, ransomware was an attack on the availability of the underlying data, where the data is encrypted by a hacker who then demands money (i.e., ransom) to decrypt the data. US CISA defines ransomware as "a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption."

> *A form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption.*

US CISA definition of "ransomware."

This “OG” form of ransomware is an attack on the "availability" portion of the CIA triad (confidentiality; integrity; availability). By rendering the data unavailable, the attacker can effectively prevent a business from operating, unless the business is able to rapidly restore the data in a known, clean environment. This can be hugely disruptive and expensive for businesses, with CISA reporting costs in the region of US$15 million for a large entity to recover from a ransomware incident. Some incidents are simply unrecoverable.


Security innovation must keep pace with innovations in ransomware technologies. Artwork by jekjob / *Shutterstock.com*

Businesses have become more adept at backup and recovery strategies to mitigate the threat posed by an encryption attack on availability of data. But attackers adapt too.

## How has ransomware evolved?

Attackers are imaginative. Availability is not the only destructive aim. As regulations that punish leaks of regulated and/or sensitive data proliferate, they create a market for attackers to demand a ransom for not exposing your data publicly. We’ve seen this repeatedly with user data, including patient health data, as well as with government and confidential company information. In the case of politically sensitive information, they might even change the leak to make it more damaging or to fuel disinformation.

As regulations that punish leaks of regulated and/or sensitive data proliferate, they create a

market for attackers to demand a ransom for not exposing your data publicly.

## What strategies are bad actors using?

Attackers often covertly steal sensitive data, then threaten victims with exposure or data breaches (confidentiality extortion) and demand a ransom for data decryption (availability extortion). The Center for Internet Security (CIS) terms this “double extortion.”

## Innovation and evolution by ransomware providers

RaaS democratizes cybercrime, escalating global data security risks with user-friendly ransomware attacks. Artwork by SpicyTruffel / *Shutterstock.com*

The ransomware threat continues to evolve. For actors wanting the “easy button,” you can buy ransomware off the shelf! Ransomware-as-a-Service (RaaS) operators provide a complete toolkit and service, splitting profit between the RaaS operator and their affiliates who trigger the attacks, making this form of attack broadly available to even unsophisticated attackers.

And the numbers are up. The *Wall Street Journal* recently reported a recurrence of ransomware related attacks and claims during the first half of 2023. Both the number of insurance claims relating to ransomware, and the total amount paid to attackers, have increased. US cyber insurance prices have continued to rise, up 11 percent year over year on average in the first quarter of 2023.

### Non-financial applications of ransomware

Some news reports on ransomware actually describe more malicious "wiper" attacks, where malware mimics ransomware not for financial gain but for data destruction, often by nation-states or political actors. These attacks, aimed at disrupting critical infrastructure like power plants or targeting political opponents, serve military or strategic purposes. A notable instance is the 2017 NotPetya wiper attack , a significant example of cyberwarfare.

## Key privacy and security regulations

### General Data Protection Regulation (GDPR)

Article 32 of the GDPR specifies "... the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk" including "the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and service" and "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident".

Thus, organizations subject to GDPR (and similar privacy regulations) that hold personal data need to implement appropriate organizational measures (i.e., internal processes on data management) and technical measures (i.e., security tooling, including privacy by design features) to mitigate against the threat of ransomware.

### Gramm-Leach-Bliley Act (GLBA)

In the United States, the GLBA specifies in *§ 314.4* the requirement to "protect against the unauthorized acquisition of customer information" which goes directly to the "confidentiality" aspect of the CIA triad. The GLBA also specifies the requirement to "Establish a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information in your control" which also covers the "availability" aspect of the CIA Triad.

### Health Insurance Portability and Accountability Act (HIPAA)

In the United States, the HIPAA specifies the Security Rule for the protection of electronic personal health information (ePHI). Specifically, per the US Department of Health and Human Services, (HHS) "the Security Rule protects a subset of information covered by the Privacy Rule, which is all individually identifiable health information a covered entity creates, receives, maintains or transmits in electronic form. The Security Rule calls this information "electronic protected health information (e-PHI)."

Since Ransomware is an electronic attack on electronically stored information, the Security rule is of primary relevance in the context of cyber-attacks. Per HHS, "The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI," and covered entities must "protect against reasonably anticipated, impermissible uses or disclosures." Given the prevalence of ransomware attacks on the healthcare industry, ransomware may be considered a "reasonably anticipated impermissible use or disclosure."

## Privacy threats and repercussion for organizations

Besides the damage to an organization’s reputation and public embarrassment, a ransomware attack and subsequent posting of confidential and personal information can result in lawsuits and penalties against the victim organization. As an example of regulatory penalties under the GDPR (in this case the UK GDPR), in February 2022, the UK Information Commissioner's Office issued a penalty against a UK law firm following a ransomware attack and data leakage.

## How to guard against data leakage and encryption

A strategy for failover and immutable backups with rapid restore capability, regularly tested, can prevent an encryption attack on the availability of data. This addresses the immediate tactical need to get a business back online quickly to help limit disruption to customers, employees, and revenue and thus ‘stop the bleeding’ during an attack.

But to prevent a “ransom by threat of disclosure” confidentiality attack, one must prevent the attacker from accessing the data in the first place. This means you need to secure all the “doors and windows” to the house. Increasingly, with cloud, this means you need to build your house securely from the start by implementing governance, enforcing requirements around credentials, encryption, and other best practices, and limiting permissions in an ongoing manner. Meanwhile you’ll want to continuously scan the environment for risks such as overly broad credentials, inappropriate role assignments, etc.


Conducting simulated phishing attacks can be an excellent strategy to build a vigilant team. Artwork by Alexandr III / *Shutterstock.com*

Mature organizations also make use of canaries, which ensure that you've implemented the controls you think you've implemented (some canaries should always fail; others should always go through). Active threat detection techniques such as workload analysis can provide early detections and warnings in the event an attacker does get "inside the house" to catch and block the attacker before they are able to encrypt or exfiltrate data.

Traditionally ransomware actors have taken a patient and stealth approach with a long "dwell-time" between first entering the environment, exfiltrating, and then encrypting data. This can be countered with early detection techniques including composite alerts, rapid and repeated scanning of environments and workloads, and tools which avoid large numbers of false-positive alerts which can swamp security teams and distract them from the most actionable and relevant alerts.

## Compliance risks and penalties for paying ransoms

Organizations that suffer a ransomware attack may out of desperation consider paying off the attacker and hope to get decryption keys back, and further hope that the attacker won't also threaten

to leak their data (double extortion). This is a risky gamble, for many reasons.

The US Treasury has published cyber-related sanctions guidance with specific instruction related to paying ransomware attackers. The US Treasury guidance states, “US government strongly discourages all private companies and citizens from paying ransom or extortion demands and recommends focusing on strengthening defensive and resilience measures to prevent and protect against ransomware attacks.” This Treasury guidance is quite clear on its face: Organizations should focus on defense and prevention of ransomware attacks using quality security tools and processes.

> If a victim pays off attackers, the victims themselves can violate US sanctions and thus become subject to US Treasury OFAC enforcement actions.

Specifically, the Office of Foreign Assets Control (OFAC) has designated many known ransomware actors as sanctioned entities or individuals. If a victim pays off attackers, the victims themselves can violate US sanctions and thus become subject to US Treasury OFAC enforcement actions. The Treasury specifically states “OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to US jurisdiction may be held civilly liable even if such person did not know or have reason to know that it was engaging in a transaction that was prohibited under sanctions laws and regulations administered by OFAC.”

Providers of cryptocurrency "mixer" (i.e., obfuscation) sites are also coming under the eye of law enforcement and are subject to criminal prosecution as well as regulatory sanctions and penalties. Such "mixer" sites are widely used to launder ransom payments, and other criminal funds, and help enable the business of ransomware.

## Relevance to privacy and compliance practitioners

From a privacy perspective, ransomware followed by a data leakage can result in violation of privacy regulations including GDPR, GLBA, HIPAA and others which require "technical and organizational measures" (per GDPR) or similar requirements under US and other laws. This is particularly true when the victim organization cannot demonstrate that it has put reasonable security measures in place to:

1. Protect against a ransomware attack, and
2. Prevent data exfiltration in the event of a ransomware attack.

Paying for decryption might be tempting, but the risk of a US Treasury investigation outweighs any potential benefits. Artwork by Chim / *Shutterstock.com*

From a compliance perspective, in the event of a successful ransomware attack, organizations may be under enormous pressure to just "pay off the attacker" to try to get their systems back up and running. However even in the best case in which the attacker provides keys to decrypt the ransomed data, the mere act of paying the attacker can lead to a Treasury investigation and potential penalties and resulting reputational damage to the organization.

## Proactive measures and continuous vigilance

For privacy and compliance practitioners, ransomware is not just "an IT problem," as the consequences can be far-reaching beyond just the technical domain. The threat is ever evolving and always looking for an easy entry point back into the former victim. Ensuring your organization has strong and comprehensive security systems, tooling, and processes in place can prevent or mitigate the impact of an attack and reduce the privacy and regulatory penalties and "clean up" required after such an event. This is truly a situation where an ounce of prevention is worth more than a pound of cure.

Disclaimer: The information in any resource in this website should not be construed as legal advice or as a legal opinion on specific facts, and should not be considered representing the views of its authors, its sponsors, and/or ACC. These resources are not intended as a definitive statement on the subject addressed. Rather, they are intended to serve as a tool providing practical guidance and references for the busy in-house practitioner and other readers.

Lea Kissner

CISO

Lacework

Lea Kissner is the CISO of Lacework and on the board of USENIX. Kissner works to build respect for users into products and systems through deeply-integrated security and privacy. Kissner was previously the CISO and head of privacy engineering at Twitter, global lead of privacy technology at Google, came in to fix security and privacy at Zoom, and CPO of Humu. Kissner earned a Ph.D. in computer science (with a focus on cryptography) at Carnegie Mellon University and a BS in electrical engineering and computer science from UC Berkeley

## Merritt Baer

Field CISO

Lacework

Merritt Baer (Twitter: @MerrittBaer) is a security executive based in Miami, FL. She serves as Field CISO at Lacework, a cloud security unicorn, and serves as an advisor to a number of young companies including expanso (container orchestration and compute at the edge, based on open source protocol bacalhau). Baer advises executives on cloud security and go to market, from Fortune 100 banks, to biotech start-ups. She also helps inform the Lacework product pipeline of security threat detection and contextualization capabilities, based on practitioner feedback and the security landscape.