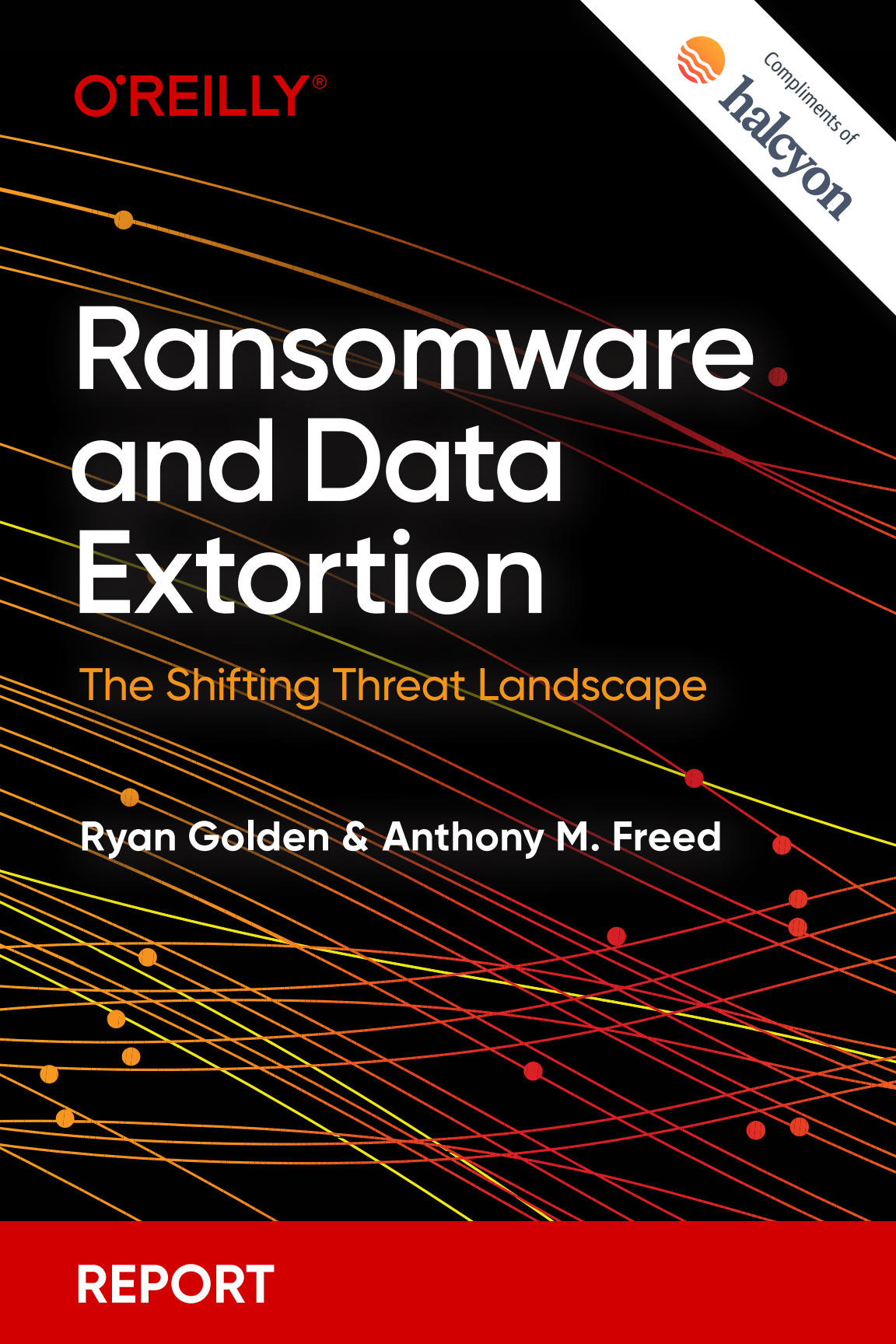
O'REILLY®
Compliments of
halcyon
Ransomware and Data Extortion
The Shifting Threat Landscape
Ryan Golden & Anthony M. Freed
REPORT

TAKE ZER0 CHANCES AGAINST RANSOMWARE

ZER0 DAYS DOWNTIME
ZER0 RANSOMS PAID
ZER0 BRAND DAMAGE

READY TO REDUCE YOUR RANSOMWARE RISK TO ZERO?
Visit halcyon.ai to learn more about the Halcyon Anti-Ransomware Platform and get a demo today.

halcyon

Ransomware and Data Extortion

The Shifting Threat Landscape

Ryan Golden and Anthony M. Freed

Beijing • Boston • Farnham • Sebastopol • Tokyo O'REILLY®

Ransomware and Data Extortion
by Ryan Golden and Anthony M. Freed

Printed in the United States of America.

Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

O'Reilly books may be purchased for educational, business, or sales promotional use. Online editions are also available for most titles (*http://oreilly.com*). For more information, contact our corporate/institutional sales department: 800-998-9938 or *corporate@oreilly.com*.

Acquisitions Editor: Simina Calin
Development Editor: Angela Rufino
Production Editor: Katherine Tozer
Copyeditor: Paula L. Fleming
Interior Designer: David Futato
Cover Designer: Karen Montgomery
Illustrator: Kate Dullea

April 2024: First Edition

Revision History for the First Edition
2024-04-19: First Release

978-1-098-16930-5

[LSI]

Table of Contents

Introduction

Ransomware is a major threat to businesses and organizations of all kinds. Ransomware and data extortion attacks are not only disruptive to business operations but also costly to resolve. They spur regulatory actions and civil litigation, including class action lawsuits against victim organizations, and more recently have even resulted in criminal charges being lodged against company officers.

Cybercriminals and hostile nation-state entities are extorting large sums from businesses and other organizations of all sizes across every industry vertical. They've been conducting such financially motivated cybercrimes for years now, continually refining and improving their exploitation techniques and encryption payloads. And even if a victim organization pays a ransom, there's no guarantee that it will actually get its data decrypted, nor is there a guarantee that its data won't be publicly exposed. Often, attackers don't reciprocate a ransom payment with the promised action. After all, they're criminals—they don't have to follow any rules but their own.

The quarterly "Halcyon Power Rankings: Ransomware Malicious Quartile" report details the most prolific ransomware groups. In the fourth quarter of 2023, these included ransomware and data extortion groups like LockBit, Play, BlackCat/ALPHV, BlackBasta, Cl0p, Medusa, Cactus, Akira, and more. While authorities have been making scattered arrests here and there, they largely have failed to stem the tide of attacks. When one ransomware gang goes down, another quickly fills the void—and often it's the same individuals. They've simply retooled and developed a new family of ransomware.

Fortunately, the news isn't all bad. Knowledge is power, and your understanding of the ransomware and data extortion threat will be a great advantage to your business. There are security controls, policies, and procedures that your organization can implement to bolster resilience and significantly reduce the risk of ransomware disruption to its operations.

CHAPTER 1

Inside the Ransomware Economy

How much money do criminals and hostile state actors make from ransomware attacks? This chapter covers some facts and figures based on recent research.

Cybersecurity Ventures's "Who's Who in Ransomware 2023" report predicts that ransomware will cost victim organizations $265 billion annually by 2031, a notable increase from the $5 billion recorded in 2017. Sophos's white paper "The State of Ransomware 2023" highlights how expensive ransomware can be. The average ransomware payment doubled in a year, from $812,380 in 2022 to a whopping $1,542,333 in 2023. And 40% of organizations that paid a ransom reported making payments of $1 million or more in 2023, compared to just 11% of organizations reporting the same in 2022.

According to ThreatDown's "2023 State of Ransomware Report", in the 12-month period between June 2022 and June 2023, there were 1,462 known ransomware attacks in the United States alone. Researchers suspect that many more attacks go unreported. Accurate data is hard to come by when assessing the wider impact of ransomware operations, as most private organizations and individuals are not required to report attacks. For example, the FBI spent seven months in 2022 observing the activities of the infamous Hive ransomware gang after infiltrating their infrastructure. The agency came to the shocking conclusion that only about 20% of attacks were being reported to law enforcement.

Ransomware accounts for 24% of overall cyberattacks on enterprises, according to IBM Security's "Cost of a Data Breach Report 2023". From that, one can conclude that ransomware is one of the most common types of cyberattacks that target businesses and institutions. The same report reveals that 27% of malicious data breach incidents were disclosed by ransomware operators versus being detected by security operations or by way of benign third-party reporting. This means that if organizations had the right solutions and strategy in place, they would have the opportunity to prevent business disruptions and the loss of sensitive data.

Let's look at who these attackers are, how they manifest in the evolving cyberthreat landscape, how they attack, and how they continue to bypass endpoint protection solutions with such ease.

Ransomware Operations Are Costly

A recent report by Chainalysis estimates that payments to ransomware operators in 2023 exceeded $1 billion, the highest number ever. It's not surprising that ransom payments have crossed this threshold. Ransomware operators run well-organized, top-down organizations akin to legitimate SaaS companies. These operations employ specialists, provide attack infrastructure services, offer tech support to the attackers and victims, engage in negotiation and money laundering, and more. These sophisticated operations have been extremely effective, and the costs to victim organizations continue to escalate.

For example, in September 2023, an affiliate of the BlackCat/ALPV ransomware group infiltrated the networks of hospitality and entertainment giant MGM. MGM's key operational systems were shut down for several days. By October, MGM's SEC filing revealed that the attack had cost the company $100 million due to operational disruptions. That of course does not include any long-term damage to the company's brand or the potential for civil litigation. While a larger company may be able to weather such huge losses, for the vast majority of organizations, an attack of this magnitude represents an existential crisis from which they may never recover.

In some circumstances, the implications of a ransomware attack can go far beyond monetary and tangential losses; sometimes attacks can jeopardize national security. For example, Johnson Controls, a major presence in the physical security and building controls market, disclosed in an SEC filing for fourth quarter 2023 that

the company had suffered losses from an attack in excess of $27 million. In addition to inflicting that staggering financial damage, the attackers also allegedly exfiltrated 27 terabytes of data, which may have exposed details for building security at the US Department of Homeland Security.

Even more recently, the Department of Defense has announced that it is investigating claims by a ransomware operator that the group exfiltrated and is threatening to leak 300 gigabytes of data stolen from defense contractor Technica that may include sensitive US military data. Attacks like these reveal the increasingly obvious overlap between cybercriminal actors and some nation-state–sponsored operations. Nations like Russia are more often leveraging ransomware operators as proxies because they allow the offending nation to maintain plausible deniability.

The Cybercrime and Nation-State Connection

Not only do ransomware operators make a lot of money from their attacks, but some of them have also been observed working directly with hostile nation-state entities. Some nations, such as Iran and North Korea, even launch ransomware and data wiper attacks directly. Nation-state threat actors are typically a part of a nation's military or intelligence apparatus. They conduct cyberwarfare against both private- and public-sector organizations. Because they're usually government trained and funded, they can use the most advanced cyberattack methods available.

In addition to often working with cybercrime groups, nation-state threat actors are known to use the same tactics. They may use the same exploit kits targeting the same vulnerabilities, as well as hijack legitimate software applications and cybersecurity tools. Recently, ransomware gangs have been observed leveraging zero-day exploits more often. These "unknown" and very valuable vulnerabilities had typically been used only in nation-state operations espionage operations. There has also been a marked increase in the use of advanced tactics like living-off-the-land (LotL) techniques, which abuse legitimate network tools for lateral movement and data exfiltration,

and methodologies like Dynamic Link Library (DLL) side-loading.[1] These used to be the purview solely of nation-state threat actors.

Ransomware-as-a-Service

You've heard of software-as-a-service, platform-as-a-service, and infrastructure-as-a-service. Well, threat actors have their spin on software-defined services too: ransomware-as-a-service (RaaS). A report from Zscaler indicates that 8 out of the 11 most common ransomware variants in 2022 were from RaaS. The situation is similar today.

The rise of the RaaS ecosystem involves multiple players who specialize in various aspects of the larger ransomware attack:

Initial access brokers (IABs)
: These highly skilled specialists are exceptionally good at penetrating and establishing a foothold within secure networks. IABs often sell access to these compromised networks to other threat actors, including ransomware affiliates. The deeper an IAB can penetrate a network, the more valuable their services become. Purchasing credentials and access is surprisingly easy and relatively inexpensive.

RaaS platform providers
: RaaS operators provide the software platform and backend to launch attacks. They have development teams that work constantly to improve their feature sets. They also assist in negotiations during a successful attack, manage customer service agents, market to new affiliates, and more—all for a slice of the profits.

RaaS affiliates
: These are the people or groups that plan and execute the actual ransomware attack. They obtain access via an IAB (or create their own), use a platform or toolkit from a RaaS operator, execute the attack, and then move the ransom monies around to stay below the radar. RaaS affiliates are some of the biggest customers of IABs.

1 DLL is a type of file that contains data resources that can be shared by multiple Windows applications.

Crypto exchange money launderers
: These people move illicit ransom payments through crypto exchanges, with the intent to hide both the origins and the destination of the funds, in exchange for a healthy fee for their services.

Command and control providers (C2Ps)
: In 2023, Halcyon researchers identified C2Ps as another major player in the ransomware economy. These are legitimate ISPs who lease the attack infrastructure to threat actors.

In many cases, the overlap between nation-state attack elements and those of cybercriminal ransomware gangs has been documented. Today's ransomware attacks are more complex and difficult to defend against than ever before.

Top Ransomware Infection Pathways

We've examined the players who engage in ransomware and extortion cybercrime, or the *who*. Now let's look at the ways attackers conduct their ransomware attacks, or the *how*. Ransomware operators and other threat actors employ a wide variety of attack vectors to infiltrate a target network. This section explores a few of the most common infection pathways.

Phishing and Other Social Engineering Attacks

Social engineering attacks are the most common ways in which ransomware threat actors get initial access to a targeted network. Phishing through malicious emails or messages on social platforms is a favorite tactic. Specially crafted emails are designed to trick targets into clicking malicious links, opening malicious attachments (which look like normal documents), or providing sensitive information like user credentials. They usually communicate urgency in their messages, for example, "This is the IRS. Contact us now or there will be criminal charges!" or "Claim the PlayStation 5 you won before we give it to another winner!" Attackers who have already successfully infiltrated a network may also use social engineering techniques to compromise identities that have more user privileges at the targeted organization, like network administrators and company executives.

Unsecured or Compromised RDP and VPN Connections

Abusing Remote Desktop Protocol (RDP) and virtual private networks (VPNs) is one of the more common tactics ransomware operators use to move laterally and vertically within a compromised network. RDP exploits are also used to remotely execute malicious code, such as by using malware or attack kits, by executing scripts in fileless attacks (malware that runs entirely in memory rather than by writing a file to data storage), or by abusing legitimate network tools in LotL attacks. Access to RDP and VPN instances is usually accomplished by way of stolen or brute-forced user credentials.

Watering Holes, Malicious Ad Libraries, and Drive-By Attacks

Lots of malware, including ransomware, is distributed through additional kinds of social engineering tactics. *Watering hole attacks* compromise legitimate websites (or fake sites that look legitimate) that are likely to be of interest to a targeted audience so they serve up malicious code. Attackers also compromise advertisement libraries in order to propagate ransomware via drive-by attacks, where the victim can be infected simply by visiting a legitimate website that is pulling in the compromised ads for display.

Tainted Software Downloads

The Kaseya supply chain attack of 2021 demonstrated that victims can be compromised by a legitimate software update from a known vendor that is signed with a valid digital certificate. This is a common supply chain exploit. Kaseya is a managed services provider (MSP), and its remote management service was exploited by the REvil ransomware gang, which in turn compromised customers around the world. REvil exploited a known vulnerability that Kaseya was just in the process of validating for a patch. Even the best security hygiene efforts cannot prevent this kind of attack from being successful. Vendors, suppliers, and clients need to collaborate on their cybersecurity strategies and engage in shared incident response as needed.

Zero-Day and Unpatched Vulnerability Exploits

Patching systems can be a complex process for some organizations. To avoid breaking critical business systems, patches often need to

be applied in development environments and tested prior to being put into production. Even then, patching may be challenging due to legacy systems and software or internal (home-brewed) scripts and applications that will break if a patch is applied haphazardly. Thus, mitigating some vulnerabilities can take months or more, leaving the organization exposed.

Brute-Forced and Stolen Authentication Credentials

As mentioned previously, attackers are keen to get their hands on stolen user credentials and often use social engineering techniques to obtain them. They can also look on dark web marketplaces for user credentials that other threat actors are offering for sale. In addition, attackers can benefit from reused credentials that have been compromised at other sites, or they can use brute-force and dictionary attacks that automate high-volume credential "guessing."

Unhooking and Bypassing Endpoint Security Tools

Ransomware attackers are adept at bypassing security controls, and endpoint protection tools are no exception. There are numerous examples of hardcoded antivirus (AV), endpoint detection and response (EDR), and extended detection and response (XDR) bypasses written into malicious code that let the attack slip by without triggering an alert. Attackers have also been observed using universal unhooking to bypass security tools. *Code hooking* is a technique used by legitimate software, including endpoint protection tools, to gain needed visibility into activity on the network. *Universal unhooking* techniques hijack execution flow, allowing attackers to deploy a rootkit, for example, and then obfuscate subsequent processes and network connections. Universal unhooking basically blinds endpoint protection tools to the malicious activity, rendering them ineffective for detecting the attack.

Network, System, and Software Misconfigurations

A *misconfiguration* is the improper deployment or tuning of software deployed in a network that leaves the tool or the network vulnerable to attack. Orchestrating all of the components of a network is a lot more difficult than it may seem and requires a great deal of skill. Minor errors in configurations can leave application instances and even the entire network exposed.

Attack Toolkits and Abuse of Legitimate Network Tools

Attackers often use legitimate penetration testing (pentesting) tools, such as Cobalt Strike and Mimikatz, to compromise a network, move laterally or vertically, steal user credentials, and more. Attackers also abuse legitimate tools that are already on the network, such as PowerShell and PsExec, for malicious activities. The use of legitimate tools reduces the likelihood the attackers will be discovered (because the tools are already trusted by security controls) and negates the need to develop additional tooling for an attack.

Dwell Time

The time that elapses between the initial ingress on a targeted network and detection of the attack by the target's security tools or cybersecurity personnel is called the *dwell time* for the attack. According to Sophos's "Active Adversary Report for Tech Leaders 2023", the median dwell time for ransomware attacks is now about five days instead of weeks. Dell Secureworks documented a case in which the time from ingress to delivery of the ransomware payload was accomplished in a matter of hours.

CHAPTER 2

Shifting Legal and Liability Landscape

So now you understand why and how ransomware is harmful, and you're acquainted with many of the cyberattack techniques that are used in ransomware attacks. It's time to examine the legal and regulatory risk your organization faces when victimized by ransomware attacks. Despite being victims, enterprises are being fined and penalized for actions taken before, during, and after successful ransomware attacks.

Regulatory Actions

Today's ransomware attacks don't simply cause operational disruptions; they most often exfiltrate sensitive and regulated data. Not only could some of your company's data become inaccessible, but it could also be disclosed publicly or sold to the highest bidder—regardless of how the actual attack is resolved.

An additional cause for concern is data privacy regulations. Although the specific regulations that apply to your organization depend on where in the world you operate, which industry you're in, and the size of your company, at least some compliance issues need to be on your radar.

In July 2023, the US Securities and Exchange Commission (SEC) announced that it would adopt new rules that require SEC registrants to disclose the cybersecurity incidents they've experienced

as well as their cybersecurity risk management, strategy, and governance strategies on an annual basis. The new rules took effect in December 2023 and apply to all publicly traded companies that operate in the United States.

Organizations must disclose "material" cybersecurity incidents within four business days, reporting them as a line item on Form 8-K. These include many kinds of events, such as data breaches, which are often the result of ransomware. "Material" may be subject to interpretation, but it's better to be safe than sorry.

But disclosing an incident to the SEC isn't the same thing as properly informing investors about how the attack may impact their investments. The SEC's new rules may pressure organizations to disclose incidents before they understand such incidents well.

Each cyberattack can impact a company a little bit differently. Digital forensics investigations can take weeks or months to conduct thoroughly. How can investors and stakeholders understand how they're impacted if the only information the organization has to share on a SEC filing is the vague "We experienced a major data breach in November 2024, and our business operations were disrupted"? Indeed, such murky reports can make investors anxious and confused. An organization can try to do the right thing by being transparent and reporting to the SEC as soon as possible. But without certainty and concrete information, an organization can unnecessarily expose themselves to additional fallout with regard to investor relations.

Moreover, regulatory actions against victim organizations and their leadership can have an adverse effect on security culture within the organizations. A punitive regulatory stance will almost certainly create top-down pressure on security teams to be less forthcoming with leadership when addressing a security event. It's not hard to see that security teams will feel pressure to not report events to leadership unless they absolutely have to, which has the potential to negatively impact security operations. All of this means that organizations that were already struggling to defend themselves against threats from ransomware and data extortion attacks now also face the threat of being revictimized by an overzealous regulatory landscape.

Many other data privacy and cybersecurity regulations exist in the United States, including the Gramm–Leach–Bliley Act (GLBA), the

California Consumer Privacy Act (CCPA), and the Health Insurance Portability and Accountability Act (HIPAA).

Paying ransoms and experiencing operational downtime can both be very expensive. But the greatest harm to your organization comes from the penalties you can incur if sensitive data is exfiltrated. The sensitive data your organization handles isn't just information about your business; it can also be sensitive information about the individuals and entities your organization does business with.

Threat of Lawsuits

If your organization's networks are struck by ransomware that conducts a data breach, it's not only the government regulators that your company should be concerned about. You should also worry about lawsuits. Data breaches expose enterprises of all kinds to massive legal liability.

For example, HIPAA requires organizations that handle sensitive medical data in the United States to protect such data from unauthorized parties. Government fines for HIPAA violations can range from $100 to $50,000 per violation, but lawsuits concerning HIPAA violations can cost millions of dollars to settle, and that doesn't include all the money organizations spend on legal fees. Logan Health Medical Center had a data breach involving patient data in November 2021 in which information on more than 213,000 individuals was compromised. Logan Health was sued, and eventually it agreed to settle for $4.3 million. Settlements like these are typical when an organization is sued by its patients, customers, or clients after a cyberattack has breached their data.

Another example is the case against QRS, an electronic health records solutions provider. According to two class action lawsuits filed in January and February 2022, QRS discovered that an unauthorized actor accessed a QRS patient portal server and may have compromised personal information stored on that server on August 26, 2021. QRS's investigation determined that the attacker first gained unauthorized access to the company's servers on August 23. Kentucky resident Matthew Tincher received a Notice of Data Breach letter dated October 22. It's alleged that Tincher's sensitive medical and personal data was exposed in the QRS breach, as was the sensitive data of about 320,000 patients in total.

Tincher is the lead plaintiff in a class action lawsuit against QRS that was filed in the US District Court for the Eastern District of Tennessee on January 3, 2022. The lawsuit filing says:

> QRS failed to reasonably secure, monitor, and maintain the Protected Health Information ("PHI") and Personally Identifiable Information ("PII") (collectively, "Sensitive Information") stored on its patient portal. As a result, Plaintiff and approximately 319,000 current and former patients of healthcare providers that utilized QRS's services suffered present injury and damages in the form of identity theft, loss of value of their Sensitive Information, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the unauthorized access, exfiltration, and subsequent criminal misuse of their sensitive and highly personal information.

A second class action lawsuit related to the same QRS breach was filed in the same court on February 16, 2022. This time, the plaintiff is listed as "K.L., on behalf of herself and all others similarly situated," and the defendants are Psych Care Consultants *and* QRS. The lawsuit filing says:

> Plaintiff brings this class action because Defendants failed in their basic, legally-bound, and expressly-promised obligation to secure and safeguard PCC's patients' protected health information ("PHI"), as that term is defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and personally identifiable information ("PII") (collectively, "Protected Information").

QRS claims that it followed procedure and complied with HIPAA by reporting the breach within 60 days of discovery. At the time of this writing, there has been little publicly available information about either lawsuit since February 2022. But what is available makes it clear that your organization can be in legal trouble in the wake of a ransomware-triggered data breach, even if you believe you're complying with data privacy laws, such as the healthcare sector's HIPAA.

Another example concerns Ultimate Kronos Group (UKG Inc.). It is one of the largest human resources and payroll technology providers in the United States. In December 2021, UKG discovered a devastating ransomware attack on its cloud payroll systems, which serve many corporate clients. A UKG representative said:

> UKG recently became aware of a ransomware incident that has disrupted the Kronos Private Cloud, which houses solutions used by a limited number of our customers. We took immediate action to investigate and mitigate the issue, have alerted our affected customers and informed the authorities, and are working with leading cybersecurity experts.

The ransomware attack put UKG's payroll systems out of service for at least a month.

The City of Cleveland is one of UKG's clients, and it believes that its employees' sensitive information was breached in UKG's December 2021 ransomware incident. Other UKG clients, Puma and the New York Metropolitan Transportation Authority (MTA), also reported data breaches related to the UKG incident. In the months that followed, employees of several UKG clients, including PepsiCo, the New York MTA, and Allegheny General Hospital in Pittsburgh, filed class action lawsuits. In July 2023, the public learned that UKG had settled class action lawsuits for $6 million. The lawsuits alleged negligence, breach of contract, and privacy law violations.

Criminal Charges

We've seen examples of the legal nightmares in civil court that can result from data breaches, which are often caused by ransomware. Now let's look at the potential criminal consequences of data breaches.

Uber

In November 2017, Uber acknowledged that threat actors had attacked the app's backend computer network in late 2016 and breached 57 million customer and driver records. The former Uber chief security officer (CSO) learned of the breach in November 2016. Under the CSO's direction, Uber made two $50,000 payments to the cyberattackers in December 2016. The CSO is alleged to have failed to disclose the incident to Uber's drivers and customers or the general public, and they made at least one of the attackers sign a confidentiality agreement. Allegedly, the CSO had not been forthcoming about the circumstances of the data breach.

In 2018, Uber paid a $148 million settlement to 50 state attorneys general because the company had failed to disclose the breach. In

2020, the Department of Justice filed criminal charges against the former Uber CSO. The criminal trial, held in the US District Court in San Francisco, began in September 2022. In October 2022, the former Uber CSO was convicted of obstruction of justice. He was sentenced to three years of probation.

The criminal charges and conviction received a lot of attention in the mainstream media, which likely harmed Uber's reputation. The former CSO's conviction also set a precedent that corporate executives can be criminally charged and convicted based on actions they take both before and after an attack that involves a data breach.

SolarWinds

Another example is the extensive attack on multiple US government departments and agencies that became public knowledge in December 2020. The SEC calls the attack SUNBURST and said it was a cyberespionage operation that Russian nation-state threat actors conducted for nearly two years. SolarWinds, which develops remote network and information technology management software, is one of the technology vendors the attack exploited in order to reach the government entities that were the ultimate targets.

In October 2023, the SEC charged SolarWinds and its chief information security officer (CISO) with fraud and internal control failures that were a major factor in the SUNBURST attack. The SEC's complaint alleges that in 2018, the CISO and other SolarWinds staff shared a finding internally that SolarWinds's remote access had poor security. Further, the complaint states that staff knew that if the software's vulnerabilities were exploited, an attacker "can basically do whatever without us detecting it until it's too late," which could result in "major reputation and financial loss." The SEC alleges that this material finding remained internal to the organization and wasn't shared with regulators or investors, constituting an SEC violation.

Gurbir S. Grewal, director of the SEC's Division of Enforcement, said:

> We allege that, for years, SolarWinds and [the CISO] ignored repeated red flags about SolarWinds' cyber risks, which were well known throughout the company and led one of [the CISO's] subordinates to conclude: "We're so far from being a security minded company." . . . Rather than address these vulnerabilities, SolarWinds and [the CISO] engaged in a campaign to paint a false picture of the company's cyber controls environment, thereby depriving investors of accurate material information. Today's enforcement action not only charges SolarWinds and [its CISO] for misleading the investing public and failing to protect the company's "crown jewel" assets, but also underscores our message to issuers: implement strong controls calibrated to your risk environments and level with investors about known concerns."

The SEC is a legal entity that's independent from criminal courts, but the agency can bring criminal cases "when appropriate". If the SEC's charges against SolarWinds and its CISO aren't criminally prosecuted, the SEC can still levy significant civil penalties against the defendants.

As of February 2024, SolarWinds has filed a motion to dismiss the SEC's complaint via federal court in Manhattan. The company believes that the SEC's complaint could make American companies more vulnerable to cybercrime because security vulnerabilities would become public knowledge as the SEC's complaint is investigated and tried.

Either way, if the SEC's allegations are true, then SolarWinds acted irresponsibly by keeping vulnerability information completely to itself. The company's legal troubles highlight the complexities of vulnerability disclosure. How should vulnerabilities be responsibly disclosed so that the impacted entities can improve their security posture, while preventing attackers from learning about the vulnerabilities before the impacted entities can harden their security? There can definitely be harsh legal penalties for C-suite executives and board members if their companies know of technology vulnerabilities without addressing them or disclosing responsibility.

CHAPTER 3

Defending Against Ransomware and Data Extortion Attacks

Considering the multitude of ways in which ransomware and data extortion attacks harm businesses financially and legally, security controls are well worth an investment of money, time, and effort. The purpose is not only to prevent attacks from being successful but also to ensure the organization is prepared to respond and be resilient should an attack be successful.

This chapter outlines a variety of security controls that, when used properly, will significantly improve your organization's security posture against ransomware and data exfiltration.

Dedicated Anti-Ransomware Solutions

Some security vendors offer advanced dedicated anti-ransomware solutions. It's worth checking them out and choosing solutions that are most appropriate for your business and its needs. Today's sophisticated anti-ransomware solutions take a multilayered approach.

Pre-execution Ransomware Prevention

As much as possible, ransomware should be stopped in its tracks before it's even able to execute. Cybercrime groups and nation-state threat actors have developed increasingly sophisticated ransomware that includes features specifically designed to evade analysis and

disable, blind, or bypass endpoint protection platform (EPP), EDR, and XDR tools.

It's possible to stop a ransomware payload at the execution phase of the attack sequence if the right tools are in place to detect it. So far, EPP, EDR, and XDR have an extremely high miss rate when it comes to ransomware.

Some commodity ransomware may be preventable with the signature- and heuristics-based tools that are used in a lot of endpoint security solutions, but as we see from the increasing number of victims daily, antivirus, detection and response, and other endpoint solutions continue to fail.

A dedicated anti-ransomware solution utilizes artificial intelligence (AI) and machine learning (ML) with behavioral analytics to identify and stop polymorphic and repacked variants of ransomware that EPP, EDR, and XDR continue to miss. This is because AI/ML endpoint protection models were trained on characteristics that all malware share, including a subset of ransomware. But ransomware does not behave like other malware, so training AI/ML models on the few characteristics that ransomware does share with other malware leaves a lot of room for missed detections. Conversely, AI/ML models in a dedicated anti-ransomware solution are trained on characteristics that all ransomware share, delivering more efficient and effective detection of ransomware attacks.

Exploitation of Ransomware Features

A dedicated anti-ransomware solution should also be designed to interrogate and exploit features that are commonly hardcoded into the dropper or payload itself. For example, a dedicated anti-ransomware solution could make it seem as though the attackers are in a virtual sandbox, where most ransomware will terminate processes to avoid analysis.

Advanced Ransomware Behavior Detections

Remember, the ransomware payload is the very tail end of a longer attack, so there are potentially days or weeks of detectable activity on the targeted network that occur long before the ransomware payload is delivered. A dedicated anti-ransomware solution should be able to detect the pre-payload activity that is most commonly associated with ransomware attacks and disrupt the operation earlier

in the kill chain—either at initial ingress, or when remote shells are launched, or when the attackers begin to move laterally on the network. A dedicated anti-ransomware solution should stop these attack progressions at the earliest stages, relegating what could have been an attack that disrupted operations and resulted in sensitive data loss to just another network intrusion attempt.

Endpoint and Network Resiliency

Effective anti-ransomware solutions have strategies for every part of the attack chain. Your solution should automate containment and mitigation of ransomware damage by isolating hosts to prevent ransomware from spreading to other devices, and by capturing key material so that data assets encrypted by the attacker can be decrypted within minutes of a successful attack. And an effective anti-ransomware solution will utilize all these layers to protect your organization at every step of the attack chain.

Patch Management

Ransomware often exploits known vulnerabilities that have available patches. It's imperative to keep all of your organization's network's operating systems, applications, and firmware up-to-date with the latest patches. You'd be surprised by how many enterprises have poor patch management. According to Ivanti's Patch Management Challenges survey, 14% of the firms surveyed incurred financial losses that might have been prevented with better patch management. Of firms responding to a Ponemon Institute survey, 74% had problems patching vulnerabilities quickly enough. The average time from a patch becoming available to a patch being installed, according to Ponemon's research, is 102 days. Ensure that the patch management process throughout your networks is automated as effectively as possible.

Data Backups

Ransomware is as much of a threat to the availability of your organization's data assets as it's ever been. Your network should automate the backup process and have human IT specialists check your backups every so often. There absolutely should be backups offsite, and it can be a good idea to keep some onsite backups as well. Thankfully, cloud platforms can make maintaining offsite backups convenient.

Access Control

Access control is a crucial pillar of cybersecurity. It's all about making sure that only authorized entities have access to particular systems and data assets. User accounts should have access only to the computing resources they require in order to perform their work; that's called the *principle of least privilege*. Today's network security must be based on the zero-trust model rather than the traditional perimeter model. *Zero-trust security* means that no user or machine is automatically trusted, regardless of its origin. An account could originate outside of or inside of your network, but it should still be authenticated at as many points as possible. Network segmentation should also be implemented to help enforce the principle of least privilege and make it difficult for threat actors to spread from one part of your network to another.

Security Awareness and Training

All people who work for your organization should receive periodic security awareness training. *Phishing* is one of the most common ways that attackers penetrate enterprise networks. Employees should be trained to identify phishing through email, social media messages, text messages, websites, and phone calls. Employees should also be taught good cybersecurity hygiene practices, such as handling their access keys carefully and effectively wiping data from old devices before disposing of them. Keep in mind, too, that if your workforce used to be onsite and has now become hybrid or remote, security awareness training needs to adapt to those circumstances. Remote workers often use their own laptop and phone endpoints to conduct their work, and if they're working from home, then they're almost certainly using their own wireless or wired local area network (LAN) in order to connect to your enterprise's network through the internet. Consider how phishing may target their home lives in addition to their professional lives. After all, cybercriminals could impersonate family members or the household utility company instead of just entities associated with the job. Security awareness training may also need to address the fact that employees may use the endpoints that are their property to play computer games or conduct their personal social media activities in addition to their work activities.

Procedure Testing

Procedure testing focuses on how your security practitioners, stakeholders, policies, and procedures enable the organization to respond to cybersecurity incidents. It is necessary to determine the effectiveness of your organization's cybersecurity incident response. Your organization may have a dedicated *incident response team* that includes people like SOC analysts, systems administrators, network administrators, CISOs, chief technology officers (CTOs), chief information officers (CIOs), and chief security officers (CSOs). Or if you're in a smaller organization, you may have a couple of IT specialists, with management making the executive decisions. Either way, have the people in your organization whose roles include responding to cybersecurity incidents or are otherwise stakeholders in cybersecurity meet from time to time. They should conduct tabletop exercises to simulate how your team would respond to different kinds of incidents, including ransomware and data breaches.

There are many great resources on procedure testing and tabletop exercises. You may want to start with the Cybersecurity & Infrastructure Security Agency's (CISA) tabletop exercise packages, which are freely available.

Resilience Testing

Like procedure testing, resilience testing is also important. Resilience testing is different from penetration testing. In penetration testing, offensive security specialists attempt to simulate real-world cyberattacks in order to find security vulnerabilities. Pentesting is very useful, but it's difficult for pentests to properly reflect real-world attacks. *Resilience testing* focuses on the organization's various security tools.

Software developers often engage in resilience testing to evaluate how their applications will perform under technologically stressful conditions. For instance, is the application designed to resist buffer overflow denial of service if an overwhelming amount of data is sent to it?

The frustrating truth is that all successful ransomware attacks bypass security solutions like EDR and XDR. So you can use resilience testing to simulate ransomware attacks against your security controls and data backup systems. Tests begin by defining scope and

objectives. Then you should identify threats and vulnerabilities. After that, you can simulate ransomware attacks according to those parameters.

Although the focus is on your technology and how it's configured, it's important to get your incident response team involved as well. Can ransomware be stopped, contained, or mitigated? Can you restore from your backups in a timely fashion? The ultimate goal is to ascertain how quickly and efficiently business operations can be restored to normal.

In order to effectively test your organization's resilience against ransomware attacks, you should consider how attackers will exploit not only software vulnerabilities but also weaknesses in your company's procedures.

Has your organization planned in detail what you'll do when cybercriminals attack? What will you do if a proper digital forensics investigation will take weeks but you need the findings now? What will you do if all of the credit card numbers in your system end up being sold by criminals on the dark web? What about all of your intellectual property and trade secrets? What will you do if hundreds of customers file a class action lawsuit? What will you do if your business partners in your supply chain are threatened? What will you do if your company gets unflattering and damaging press in news headlines around the world?

Have you planned for all the contingencies? Have you considered the worst possible scenarios? You need to get all of your stakeholders on board and put your full efforts into frequent resilience testing. Test many different facets—technological, operational, and legal. Based on the findings of your tests, you can make improvements to your organization's security posture against ransomware.

Conclusion

So now you understand how ransomware and data extortion attacks have a profoundly negative impact on business. Such attacks are quite common, and they can cost your company over a million dollars per incident. Then there are all sorts of other factors that can harm your business, from civil litigation to criminal charges to reputation damage.

Cybercriminals and nation-state threat actors use a variety of techniques to extort money from businesses. And by leveraging IABs and RaaS, attackers can do tremendous harm without having advanced technical skills.

But all hope isn't lost. There are many ways your enterprise can greatly improve your security defenses to lessen the likelihood and impact of ransomware attacks. These include not only advanced anti-ransomware software but also corporate policy, employee training, and careful planning.

Now that you better understand the ransomware and data extortion threat, your business is ready to do something about it. Some investment of time and resources will pay off many times over in the savings your company will realize from better cybersecurity.

About the Authors

Ryan Golden has a strong background in marketing and leadership roles across the security industry and is currently serving as the CMO at anti-ransomware innovator Halcyon. Prior to that, Golden worked as the Vice President of Marketing at ShiftLeft, Inc. Ryan has significant experience in building successful brands, as demonstrated by his role as VP of Design & Creative at Cylance, Inc., where they developed and built the disruptive Cylance brand from pre-revenue to a $1.4B acquisition by BlackBerry. Golden is a technical CMO with deep experience in defending organizations against ransomware operations and other advanced attack scenarios.

Anthony M. Freed is a strategic communications leader who is director of comms and threat research at Halcyon. Freed is an award-winning writer and producer who was previously a freelance security journalist who authored ground-breaking investigations, is a keynote speaker and presenter at major security conferences, moderated the Cybersecurity Forum Panel at the 2016 Republican National Convention, was a member of the U.S. Security Journalist Delegation to Israel, has authored multiple articles for professional academic publications, is an ambassador for Hacker Highschool, and is communications advisor at Cyber Security Forum Initiative. Freed is also the principal researcher who produces the quarterly Halcyon report "Power Rankings: Ransomware Malicious Quartile - Inside Data Extortion Attacks."