CAPINTECH

The Current State of Ransomware

By Allison Davis Ward, Partner

The dreaded ransomware. At this point, we've been inundated with news of ransomware impacting our communities, and many of us have experienced it or know someone who has. As the headlines demonstrate, no organization, industry, or government is immune, and the effects are widespread.

The ransomware industry is here to stay. If people didn't pay the ransom, the industry would cease immediately. However, bad actors can be extremely successful at receiving payout, and that stems from the underlying duty of an organization to protect its constituents and provide them with service. Depending on your preparation and ability to detect and respond to an incident, if your organization falls victim to an attack, you may be forced to make a very difficult decision between paying the ransom or not.

Organizations can't ignore the threat of ransomware in the hope that it will go away. There's a significant chance that your organization will be affected by ransomware at some point. That's why it's important to remain knowledgeable about the state of ransomware: what the current threats are, how it has evolved, and what we can expect in the future. From there, you can be proactive in evaluating your existing controls and determining where enhancements are needed.

Start with an understanding of the basics of ransomware and baseline controls, which we explain here. Now let's take a look at the current state of ransomware, including risks and the potential impact.

3 Key Takeaways About Ransomware

Ransomware could be discussed for days on end, but we see three primary takeaways from recent events.

1. The impact is long, and it only grows.
In the past, ransomware resulted in data being encrypted. If organizations didn't have thorough, recent backups to restore from, they faced either permanently losing access to their data or paying the ransom in the hopes of regaining access, which is never guaranteed. However, the impact of ransomware has become increasingly long — and it's about more than just getting your data back.

Ransomware now typically involves double extortion. During an attack, the ransomware enters your network and encrypts data, disrupting operations and services. Ransom is demanded for recovery.

But it doesn't stop there.

Your data won't only be encrypted – when the ransomware infiltrates your network, it will first exfiltrate your data. Now you either pay, or you choose not to pay and restore from backups. But either way, the bad actors will likely extort you again and demand payment to prevent them from publishing the data they exfiltrated.

And that double extortion can sometimes become triple extortion. The bad actors may not stop with you — they often go to your constituents and partners and demand payment from them related to the information that was exfiltrated. They may threaten your management, executives, and board. The opportunities for the bad actors go on and on.

However, the impact can extend past the ransom demand. Organizations that suffer a ransomware attack can lose intellectual property, incur financial losses due to penalties or fines, and experience the loss of constituents' trust. Nonprofits may also lose donors' trust.

Organizations can also lose talent. According to Cybereason's Ransomware: The True Cost to Business report surveying organizations that had experienced a ransomware attack, 32% reported losing C-level talent as a result of a ransomware attack, and 29% had to lay off employees due to financial pressures stemming from the attack. This is significant — replacing high-level talent can cause disruption and expense for an organization.

As you can see, the collateral damage is not minimal and there are far-reaching impacts. But how is that quantified?

The impact of ransomware has become increasingly long.

Sophos surveyed over 5,000 organizations of various industries, sizes, and complexities for its April 2021 State of Ransomware Report, which provides insight into the financial cost of ransomware incidents. The survey found that the average total remediation cost more than doubled over the prior year, from $0.76 million to $1.85 million per ransomware event worldwide. **In the United States, the average remediation cost was $2.09 million per ransomware event**. While there are many other factors and considerations, such as the type of industry and nature of the attack, the statistics reiterate that the impact of ransomware is significant — and growing.

2. Ransomware doesn't just target organizations with sensitive or critical data.
The attacks on the Colonial Pipeline Company and JBS Foods showed that bad actors aren't just targeting companies with sensitive data. Yes, the encryption and exfiltration of sensitive data is a prime reason many organizations choose to pay, even though you can't trust a bad actor's word that they will unencrypt your data and won't release it on the dark web. And it's why bad actors target financial, legal, higher education, and healthcare institutions. But ideal targets for ransomware now extend far beyond those that have sensitive or critical data.

If you have operations that you want to keep up and running, you are an ideal target for a ransomware event. If an organization feels it has a duty to its constituents and partners to provide critical services, there is a higher chance they will do what is required to get back up and running as quickly as possible —and sometimes they determine that what is required is paying the ransom.

That's why Colonial Pipeline CEO Joe Blount decided to pay. Blount testified to the Senate Homeland Security Committee that he felt restoring the pipeline, which is a critical infrastructure asset, "was the right thing to do for the country."

And in the healthcare and similar industries, there are operational concerns on top of the risk of data exposure. If a healthcare entity's operations are shut down, it could become a life-and-death matter for someone who is receiving critical care or lifesaving treatments.

It's vital to evolve your controls to not only allow you to recover from an incident but ensure that you are as equipped as possible to prevent it from occurring or spreading.

The takeaway here is simple: no one is immune. If you have data that you want to be available or if you have services and processes that you want to keep operational, you need to protect your organization.

3. Controls need to evolve with the threats to balance prevention, detection, and response.
Some organizations may feel that if nothing has happened to them yet, it must mean their controls are sufficient. Many organizations also believe that if they have backups to recover from or cyber insurance to help them recoup losses, the impact from ransomware will be minimal and they can recover. But it's important to remember that restoring from backups is not always a quick process, depending on how many systems were affected, and insurance doesn't cover damage to your reputation.

As we noted above, there are significant impacts even if you can recover from a ransomware incident. And just because an incident hasn't plagued you now, it does not mean it won't in the future. It's vital to evolve your controls to not only allow you to recover from an incident but ensure that you are as equipped as possible to prevent it from occurring or spreading. You must continually reevaluate the risks and the sufficiency of your controls in mitigating them.

So, what controls should you be considering in your environment? This article explains the evolving controls that your organization can implement to help you mitigate the risks and impact of ransomware.

Questions? We're here to help! Please contact us at cybersecurity@capincrouse.com.

Additional Resources:

Understanding Ransomware: Malware in Its Cruelest Form

How to Take Your Ransomware Controls to the Next Level

The State of Ransomware and Enhanced Controls Recorded Webcast

About the Author

Allison Davis Ward, Partner
CapinTech
award@capincrouse.com
o 505.50.CAPIN ext. 2008

Throughout her time as an information systems auditor, manager, and partner, Allison has provided information security assessment and consulting services primarily for nonprofit organizations, financial institutions, and health facilities. In addition to these services, she has provided clients with consulting services in risk assessment and policy development engagements.

About CapinTech

Capin Technology, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to financial institutions, nonprofit organizations, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessment, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at capintechnology.com.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.

AN INDEPENDENT MEMBER OF BDO ALLIANCE USA