statecollectionservice.com

CYBERSECURITY RISK MANAGEMENT

Protocols to Appropriately Manage Cyber Threats

INTRODUCTION

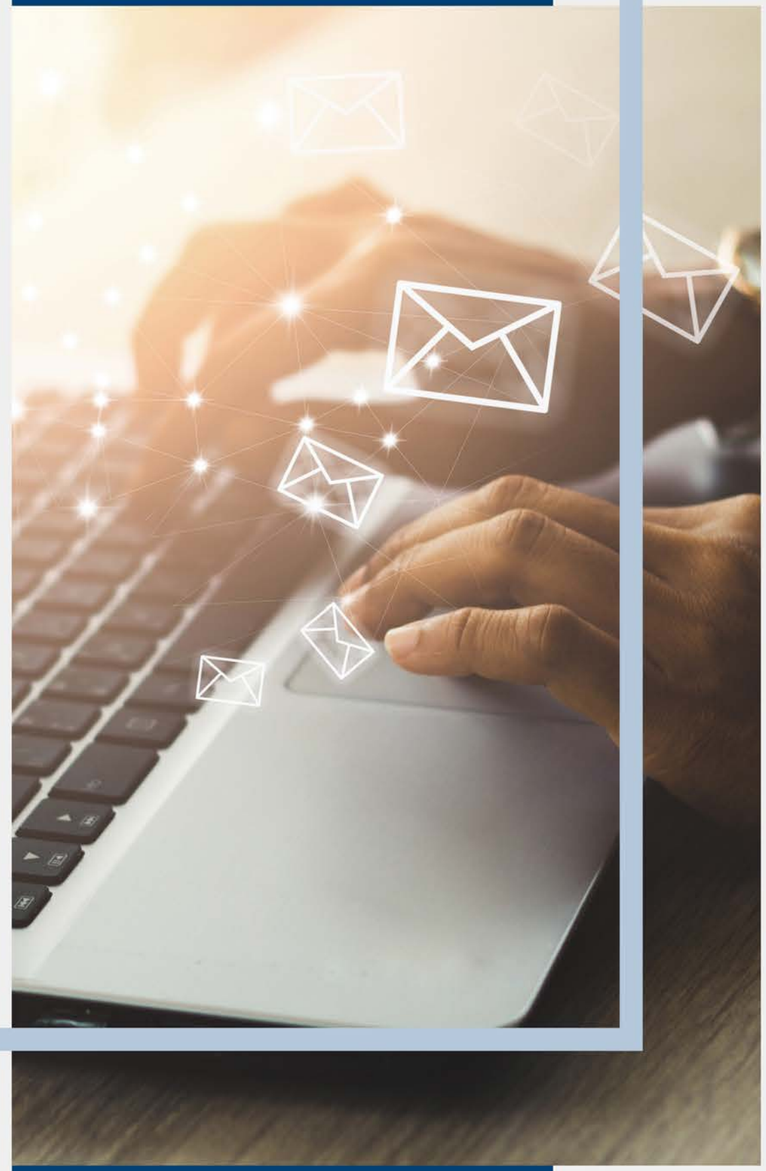
Sadly, cybersecurity incidents will continue to rise. Rise in terms of frequency, cost, complexity, and invention of new methods. The result is greater risk, increased premiums, deductibles, restrictions, exclusions, and scrutiny of your security program. However, there are several effective protocols we can implement to mitigate this dreadful threat by continuously evolving cybersecurity and risk management programs.

Here are a few trends to watch according to a recent article in **Insurance Business America:**

- Ransomware losses have dropped in the past few months, but increased in severity with ransomware-as-a-service on the rise.
- Social engineering fraud has outpaced ransomware.
- Changes to the threat landscape will introduce stricter data privacy and breach notification regulation.

While a broad topic, this whitepaper will focus on the investment in a few security protocols to help mitigate cybersecurity risk.

“How can we assess the risk and align that with the coverage in place and the processes that contribute to keeping cybersecurity risk in check,” asks Kris Aeschlimann, State’s chief financial officer.



OVERVIEW

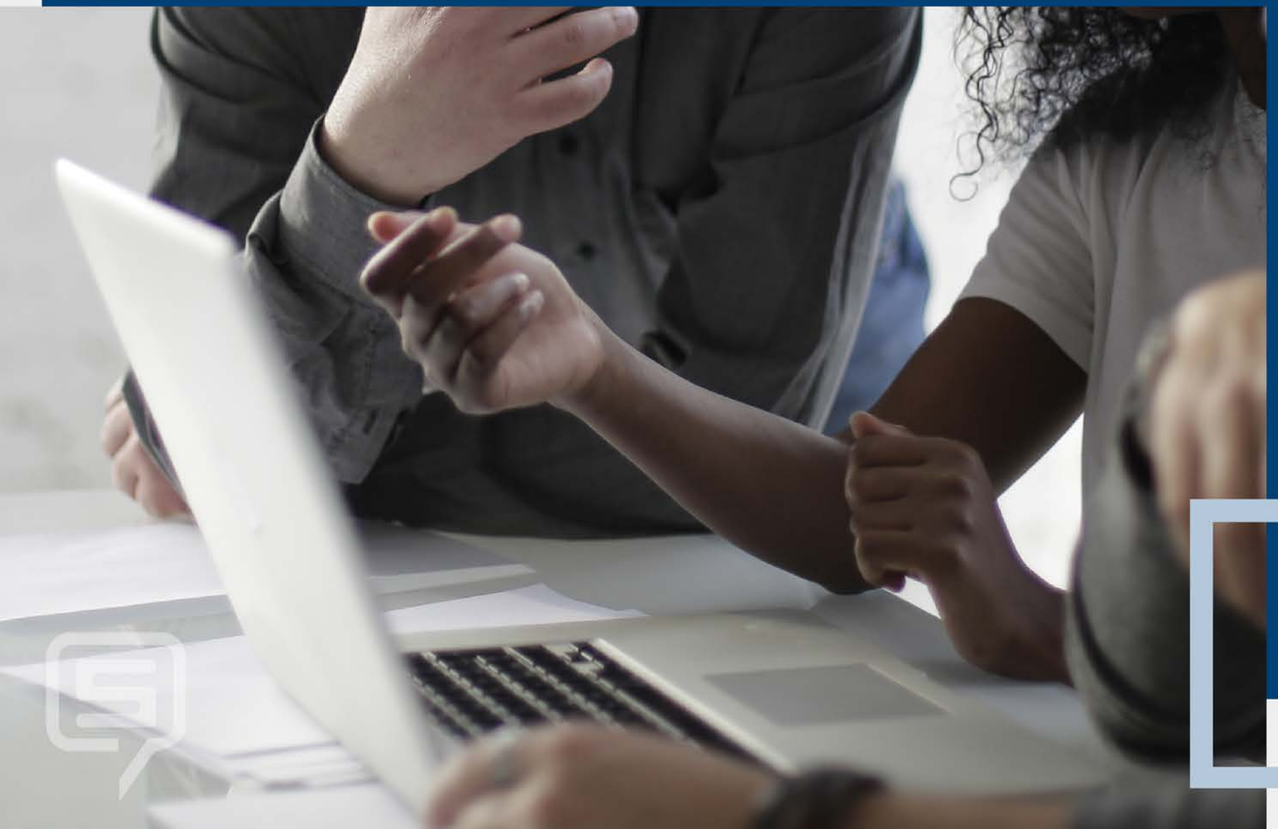
Ransomware is still the favorite attack technique to obtain PII, PHI and other sensitive data, doubling in 2022 from 2021. Acronis revealed in its latest Cyberthreat Report that global ransomware damages are expected to exceed $30 billion in 2023. In addition, the FBI reported that business email compromise scams have increased by 39% since 2020, contributing to $2.4 billion in annual losses and costing an average of $120,000 per incident. Ransomware experienced a $352,000 loss on average.

Nobody is immune from an assault, which makes it even more important to not rest thinking your cyber liability insurance coverage alone is enough. The cyber insurance market is toughening underwriting, restrictions, and security standards due to this increasing risk and cost of an incident.

"In today's digital world, it is essential for organizations to evaluate their cyber risks in order to protect their data and ensure the security of their operations. Without proper evaluation and mitigation of cyber risks, organizations are vulnerable to malicious attacks and data breaches that can have devastating consequences. Insurance is only protecting the aftermath, not preventing the damage. State has been an industry leader in implementing proactive strategies across all their platforms," explains Chris Fereday, president of PDCM Insurance.

What are some key factors to better prepare you to combat security threats?

A CULTURE OF SECURITY AND PRIVACY



Working together to continuously improve creates a strong culture, whether we're talking security and privacy or any other business issue. It is important to gain a clear understanding of the critical assets to continue operations through adverse events.

A CULTURE OF SECURITY AND PRIVACY

Security and privacy policy and procedures should aim to care for sensitive data and systems. Since humans are the weakest link, it is essential to continually educate employees at all levels of your organization.

For example, State frequently runs simulated phishing campaigns because email is the largest attack vector in most organizations. Team members who click on a link during a simulated campaign are provided with additional training on how to avoid being a victim. Repeat offenders are subject to disciplinary measures, including termination when necessary.

State also invests heavily in advanced threat protection technologies to safeguard our perimeter and every endpoint.

PARTNERSHIPS FOR A LIFETIME

It is valuable to know the security posture of your third-party business partners. Do you have an inventory of all business partners and regularly assess their security risk? What security compliance frameworks do your business partners employ and are regularly audited against? Do you know who has access to sensitive data or systems?

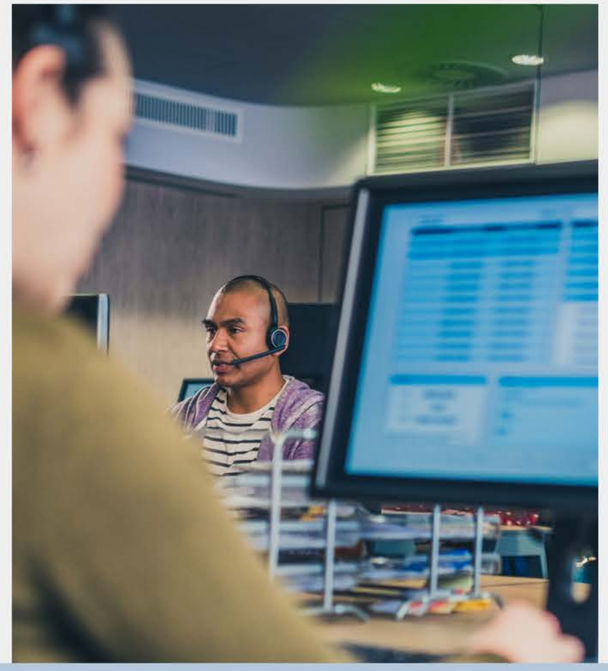
PARTNERSHIPS FOR A LIFETIME

Using a framework to assess actual risk will be far more beneficial in protecting your sensitive data than simply mandating a dramatically increased cybersecurity policy.

State recently invested in certification against the Health Information Trust Alliance (HITRUST) Common Security Framework® (CSF). HITRUST provides State with an information security framework that enhances existing, globally recognized standards, regulations, and best practices.

As has been the case for many years now, State continues to lean on our security partner for both audits by an independent, qualified assessor and continuous compliance against important standards, regulations, and laws of HIPAA, PCI DSS, and ISO 27002.

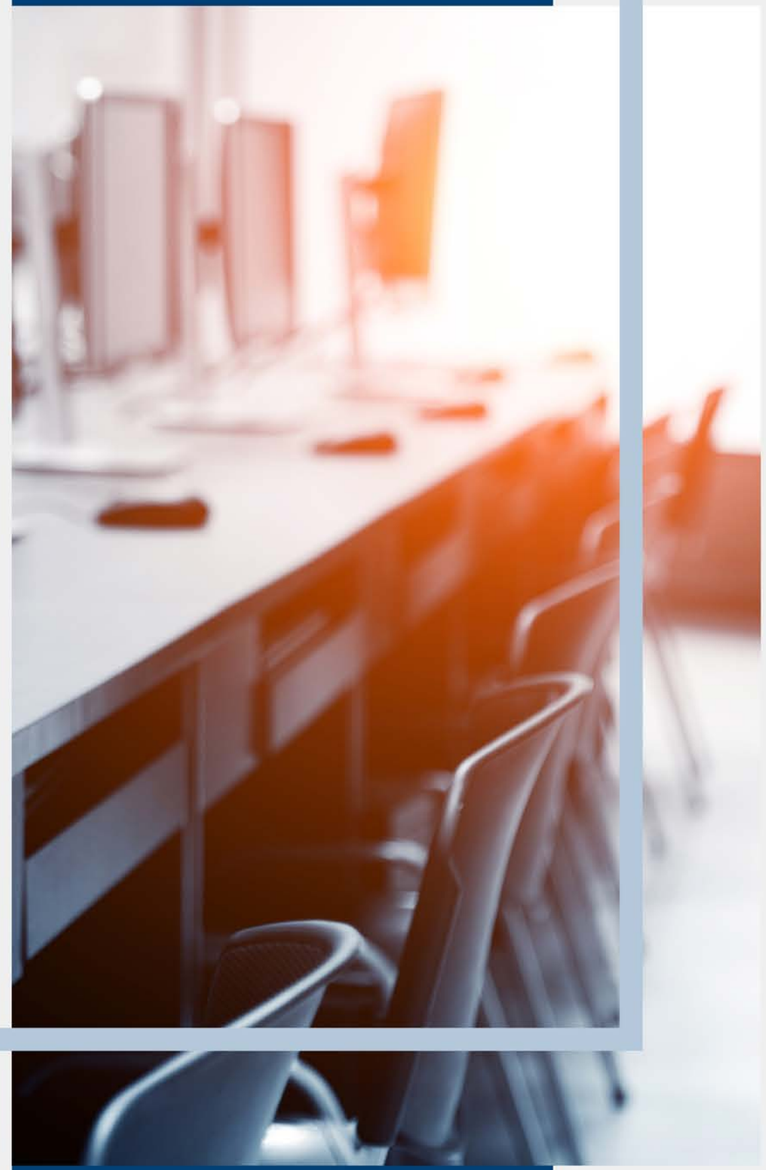
PLAN AND ASSESS



A crisis is chaotic, and even more so if you don’t have a plan or conduct exercises on a regular basis. Update your plan regularly. Test and retest.

It’s easy to overlook but ensure your cyber policy partner works in combo with your incident response plan. Do you know when and how to involve your cyber insurance partner?

At State, we recognize the need to mitigate, adapt, and respond to the “when.” As a result, we invest significant resources in regular tabletop exercises and scenarios to prepare in advance. This ensures every member of the response team knows what is expected and can tackle potential roadblocks.



TAKEAWAY 1

CREATE A CULTURE OF SECURITY AND PRIVACY

Security does not exist in a vacuum. The work to continuously improve security posture matters. A great deal.

TAKEAWAY 2

KNOW YOUR BUSINESS PARTNERS

As we adopt new technology to improve our business and our lives, it becomes even more important to ensure a culture of security, deeply understand your business partners, and work tirelessly to improve your security and privacy program. It takes an iterative team approach of strength, purpose, and perseverance to fight the good fight.

TAKEAWAY 3

CONTINUOUSLY IMPROVE YOUR SECURITY AND PRIVACY PROGRAM

Tim Haag, State's President sums it up well, "At the end of the day, we are serious about our investment in security and privacy compliance programs, technology, as well as our partners, to better combat this serious business risk."

CONTACT US

JIM WARNER, CHIEF SECURITY OFFICER
STATE COLLECTION SERVICE

PHONE
800.477.7474

WEBSITE
statecollectionservice.com

EMAIL
learnmore@stcol.com

ABOUT STATE

State improves the financial picture for healthcare providers by delivering increased financial results while ensuring a positive patient experience. Rooted in a tradition of ethics, integrity and innovation since 1949, State uses data analytics to drive performance and speech analytics with ongoing training to ensure patient satisfaction. A family-owned company now in its third generation of leadership, State assists healthcare organizations with services spanning the complete revenue cycle including Pre-Service Financial Clearance, Early Out Self-Pay Resolution, Insurance Follow-Up and Bad Debt Collection.

To learn more about how State's security protocols benefit our healthcare provider partners, email learnmore@stcol.com.