



2022



The Cyber Insurance Landscape: **Yesterday, Today, and Tomorrow**

A Collection of Perspectives from Subject Matter Experts



Table of Contents

- 03** **Introduction and Author Features**
By Cowbell
- 04** **Improving the Nation's Information Security Through Growing Community**
By Stan Stahl, PhD, President, SecureTheVillage and Director of Information Security, Miller Kaplan
- 06** **Beyond Cyber Insurance: The Importance of Employee Training and Education**
By John Iannarelli, FBI Special Agent (Ret.), Cybersecurity Speaker, Author & Consultant
- 08** **Consumers Can Help Mitigate their Exposure to Identity Theft**
By Mark Pribish, Practice Leader, Identity Theft and Data Breach Solutions Vero, A CU Direct Company
- 10** **Recent Evolution of Ransomware and Business Email Compromise Events***
By Jennifer Coughlin, Partner, Mullen Coughlin LLC
- 13** **Combat Ransomware through Resilient Backups**
By Jeff Reichard, Vice President, Public Sector & Compliance Strategy, Veeam Software
- 15** **Reduce Your Cyber Liability with Preemptive Email Security**
By Shalabh Mohan, Head of Product, Cloudflare Area 1
- 18** **An Investor's Perspective on the Future of Cyber Insurance**
By Victoria Cheng, Partner, PruVen Capital
- 20** **Cyber Insurance: How Policyholders Can Mitigate Their Own Cyber Risk**
By Isabelle Dumont, SVP Marketing and Technology Partners, Cowbell

Cowbell is signaling a new era in cyber insurance by championing adaptive cyber insurance. Adaptive cyber insurance coverage follows the policyholder's cyber risk exposures as they evolve. Continuous risk assessment keeps the policyholder and insurer up-to-date with risk profile changes. Continuous underwriting enables adjustment of coverage to account for changes in one's risk profile. Continuous risk monitoring enables the policyholder to remediate newly identified risk exposures to stay safe. All told, benefits of adaptive cyber insurance reach policyholders, risk bearing entities and brokers alike.

Just as the concept of adaptive cyber insurance connotes dynamicity and an ever-changing environment, so too does this e-book as it includes a variety of perspectives on the cyber insurance landscape, its evolution over time and predictions for the future. Guest authors bridge the gap between the insurance and cybersecurity fields, public and private sectors, as well as both sides of Cowbell's business.



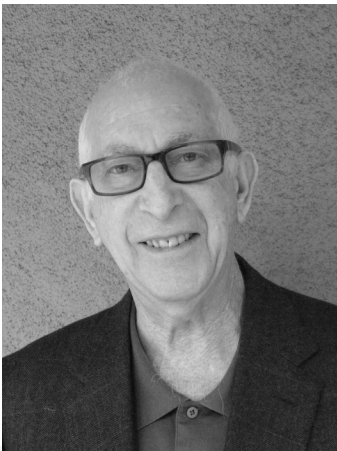
The following chapters feature the authors below:

- **Stan Stahl** articulates the view that we all have a personal responsibility for data care and information security. It truly takes a village to improve the nation's information security.
- **John Iannarelli** underscores the intersection of cyber insurance with cybersecurity and the importance of cyber education.
- **Mark Pribish** explains the complexities of identity theft and how cyber insurance responds to the identity theft and data breach epidemic.
- **Jennifer Coughlin** provides her perspective on the evolution of cyber incidents and how cyber insurance is playing a role through incident response.
- **Jeff Reichard** explores the topics of ransomware and backups through quantitative data.
- **Shalabh Mohan** suggests grappling with the importance of email security as a proactive way of stopping ransomware before it even hits your inbox.
- **Victoria Cheng** comments on the future of cyber insurance and why her company invested in Cowbell.
- **Isabelle Dumont** seeks to empower policyholders to take cyber risk management into their own hands through adaptive cyber insurance.

Chapter One

Improving the Nation's Information Security Through Growing Community

By Stan Stahl, PhD



Stan Stahl, Ph.D.

President, SecureTheVillage

Director of Information Security, Miller Kaplan

Dr. Stahl is the founder and President of [SecureTheVillage](#), a 501(c)3 non-profit on a mission to educate, support, and advocate for cybersecurity and data privacy. SecureTheVillage connects cybersecurity and privacy leaders, creating communities of interest to accelerate progress toward a secure global village. SecureTheVillage is a proud member of Nonprofit Cyber, the first-of-its-kind coalition of global nonprofit organizations to enhance joint action to improve cybersecurity.

Dr. Stan Stahl began his information systems security career in the 1980s as a research scientist at MITRE, going on to secure Top Secret teleconference and database systems for the White House, Cheyenne Mountain, and America's nuclear weapons arsenal. In 2002 Stan founded Citadel Information Group — now part of [Miller Kaplan](#) — to bring sound information security management practices to midsize and smaller organizations

Dr. Stahl has a long history of community service. He currently serves on the Small Business Advisory Council of the Cyber Readiness Institute, the Advisory Board of US Valor, and the Advisory Board of Los Angeles Cyber Lab.

Dr. Stahl earned his Ph.D. in mathematics from The University of Michigan. He is the author of [The Agnostic Patriot: A Citizen Searches for the Soul of America](#).



Stan Stahl, PhD

Improving the Nation's Information Security Through Growing Community

Author William Gibson wrote *the future is already here—It's just not very evenly distributed*. The same is true in information security and privacy management. The federal government, our think tanks, our universities, private sector companies, and many others continue to advance the state of the practice while mid-size and smaller organizations, along with individuals and families, continue to fall behind. Data care, cybersecurity, and privacy management are not evenly distributed.

The result is an ecosystem of “*cyber-haves*” and “*cyber-nots*,” with the *cyber-haves* possessing the managerial knowledge, the staff, and the financial resources to adequately protect themselves while the *cyber-nots* lack the knowledge, staff, and resources to protect themselves against an increasing volume of increasingly sophisticated cyberattacks.

The inability of the *cyber-nots* to adequately secure the data and information in their systems represents significant danger to the nation and our economy, given that the *cyber-nots* account for somewhere around half of GDP. Since these mid-size and smaller organizations are often supply-chain partners to the larger *cyber-haves*, their security shortcomings also increase the cyber risk of these larger companies. When coupled with the reality that we face a severe cybersecurity workforce shortfall numbering over 500,000 unfilled positions, it's clear that we have a national imperative to find creative ways to improve the nation's cybersecurity capabilities.

So how do we do it?

Thirty-five years ago I was a security engineer for aerospace giant TRW having lunch with my boss, a man named Frank Quigley. Frank had retired as a Navy crypto commander and now was head of much

of TRW's information security work for the Department of Defense (DoD). As the salami for our sandwiches was being sliced, Frank said “This is how we have to package information security. We need to be able to sell a customer ¼ pound of security or 1 ½ pounds, whatever he needs.”

In the 35 years since Frank said that we've pretty much learned to deliver information in the “slices” that he talked about. The challenge now is to put more nutrition in each slice.

This is what collaboration, community building, and the breaking down of barriers can do. To the extent those of us who deliver information security and privacy work together to help the *cyber-nots*, they get more nutritional value in our combined efforts. When the CEO is given the same advice by his cyber-attorney, his MSP, his virtual-CISO, and his insurance broker, the impact is far more powerful than any individual perspective.

Nonprofit Cyber is a coalition of implementation-focused cybersecurity nonprofits who collaborate, voluntarily align activities to minimize duplication and increase mutual support, and link the community to key stakeholders with a shared communication channel. The result is that *Nonprofit Cyber* members become more cost-effective in providing education, support, and advocacy to the *cyber-nots*. We do more with less, providing more security nutrition in each slice of lunchmeat.

SecureTheVillage, through our *LA Cybersecure* program, is bringing together the local information security professional community along with other national and regional cyber leaders to make a measurable difference in the security capabilities of our city's *cyber-nots*.

Collaboration, community building, and the breaking down of barriers. This is what makes $1 + 1 = 1,000$. By bringing together the “security value” of individual community members, we grow our collective security value nonlinearly. This is how we make cybersecurity and privacy more evenly distributed.

Chapter Two

Beyond Cyber Insurance: The Importance of Employee Training and Education

By John Iannarelli



John Iannarelli

FBI Special Agent (Ret.), Cybersecurity Speaker, Author & Consultant

John Iannarelli was an FBI Special Agent and served as the FBI's national spokesperson. His investigative work included the Oklahoma City Bombing, 9/11 Attack, shooting of Congresswoman Gabrielle Giffords, and the Sony hack. He is the recipient of the FBI Director's Distinguished Service Award, as well as an Honorary Doctor of Computer Science. After retiring from the FBI, John was an NFL Security Representative, overseeing game-day security of players, fans, and the stadium throughout the football season and during the Super Bowl.

John is a former police officer, attorney, author of five books and a highly sought-after keynote speaker who has presented to Fortune 500 companies, domestic and international audiences, the United Nations, and the Vatican, where he has personally met on several occasions with Pope Francis.

<https://FBIJohn.com>



John Iannarelli

Beyond Cyber Insurance: The Importance of Employee Training and Education

Today's businesses must exist in the cyber world, which means companies rely upon email, websites, and computer networks to conduct operations. This also means that businesses can be hacked, resulting in both sensitive data and money being stolen. Because cyberattacks continue to increase every year, it is essential for companies to employ best cyber practices to protect themselves. Some cyber insurance providers support this type of preventative behavior by providing educational cybersecurity resources and services.

[Cell phones](#), web access, data storage, and other every-day technology have made businesses vulnerable to cybercriminals targeting proprietary information and money. Small and medium-size businesses are especially vulnerable because cybercriminals know smaller-scale operations have fewer available resources to combat these attacks. Additionally, recovering from a cyberattack necessitates the added cost of hiring computer professionals to fix the problem, along with attorney fees to defend against lawsuits, and regulatory fines for what might have otherwise been avoidable compliance failures. Furthermore, reputational damage can impact the company's ability to conduct future business. To protect against a cyberattack, businesses must understand the risks, as well as educate their employees and customers about them.

Phishing is a common cybercrime where the cybercriminal sends an email with links or attachments that, when clicked on, download malware onto the computer system. The malware can then allow cybercriminals to access sensitive data from the company's network, such as bank account information, credit card numbers, and private email messages. An employee trained to first think before they click can be the best defense against a malware attack.

Business Email Compromise involves a cybercriminal hacking into the company's network to review business emails. Upon determining who handles the company's financial transactions, the cybercriminal will impersonate a vendor awaiting payment and provide false wiring instructions. Having cyber protocols in place that govern how money is paid based on email requests can prevent the company from becoming a victim.

Additionally, all businesses should employ basic technology defenses, including secure firewalls and web filtering software to prevent employees from accessing nefarious websites. Although such steps cannot eliminate every cyber risk, these efforts can greatly reduce the likelihood of an attack being successful and make the business a less attractive target, causing the cybercriminal to look elsewhere for another victim.

All these efforts require education. Time should be set aside on a regular basis to educate and remind employees of the cyber threats and the steps they need to take to keep the business safe. Additionally, customers who conduct business online with the company should also be warned against the threats, and how they too can avoid becoming a victim. Training the employees will protect the company's bottom line while educating the customer will protect the brand.

Just as businesses rely upon the Internet to conduct operations, cybercriminals target businesses that ignore cyber exposures. By understanding and educating employees and customers alike about these risks, companies can reduce their vulnerability and focus instead on their businesses.

Chapter Three

Consumers Can Help Mitigate their Exposure to Identity Theft

By Mark Pribish



Mark Pribish

Practice Leader, Identity Theft and Data Breach Solutions
Vero, A CU Direct Company

Mark Pribish is the Practice Leader for Identity Theft and Data Breach Solutions at Vero, A CU Direct Company in Scottsdale, Arizona. Mr. Pribish has 32 years' experience in the identity theft services, cyber insurance and data breach risk management business sectors. He is the author of the longest running monthly ID Theft column in the United States.

Mr. Pribish is a member of the Identity Theft Resource Center Board of Directors, Grand Canyon University Technology Advisory Board, Arizona FBI InfraGard Public Private Alliance, and FBI National Citizens Academy Alumni Association. Prior to joining Vero, he held senior level positions at MIS, Aon and AIG. He is a graduate of the University of Dayton.



Mark Pribish

Consumers Can Help Mitigate their Exposure to Identity Theft

Most consumers think of cyber insurance as protecting a business only. However, it can also help protect the consumer in the event of a data breach incident.

A primary purpose of cyber insurance is to provide finance coverage and help businesses recover from a cyber incident, whether it be a data breach, a business email compromise, a ransomware attack, and even an insider threat (e.g., current and former employees, contractors, and vendors).

Cyber insurance can also help the consumer when a business experiences a data breach incident by responding to notification costs to “affected” individuals along with credit monitoring costs to help mitigate an individual’s risk of becoming a victim of identity theft. That said, individual consumers should not wait for their Personally Identifiable Information (PII) to be “lost or stolen” from an organization’s data breach incident.

Instead, consumers or businesses can protect themselves and their personal privacy by being proactive and prepared to reduce their exposure to the everyday risks of identity theft with my top 10 tips to reduce their risk of identity theft including:

Personal privacy

1. Be more vigilant and read the terms and conditions of your app and social media accounts, use the privacy settings of your accounts, and be cautious about your social networking.
2. Be aware that fake social media accounts are on the rise, from name brands to famous people to the average person where scammers depend on human nature, psychology and “trusting” consumers to let their guards down.

3. Know that scammers are targeting young adults, remote working employees and the elderly through email, regular mail and the telephone.
4. Read and understand the privacy policies of every organization you have a relationship with to know how your information is protected, saved, analyzed, sold and/or disclosed.

Identity theft

5. Synthetic-identity theft and fraud are emerging threats. Check your credit-bureau report quarterly.
6. While no password is “unbreakable,” do not make it easy for identity theft criminals by using weak or repeated passwords. Instead, use a “pass phrase” of 21 characters or more.
7. The best defense against phishing is to be aware that it happens every day. Assume you are being “phished” until you verify the source of an unexpected email or call.

Cybersecurity

8. Consumers need to understand that every business they have a relationship with is at risk of a data breach incident and that a data breach is inevitable.
9. Consumers need to be more cautious in sharing personal data with organizations, such as loyalty cards where personal information is sold repeatedly to marketing organizations.
10. Personal computers, phones and smart home devices of consumers present a risk in that hackers can steal identities. Personal cyber insurance may be a good option.

Increased education and awareness will help consumers be better prepared against the everyday challenges of the Phishing (fraudulent emails), Vishing (fraudulent phone calls and voicemail messages) and Smishing (fraudulent text messages) tactics of hackers and ID theft criminals.

To conclude, do NOT let your guard down. Always be cautious in revealing information about yourself or your employer. Always “stop, look and think” about emails, texts, and phone calls. Always slow down, be aware and be safe.

Chapter Four

Recent Evolution of Ransomware and Business Email Compromise Events*

By Jennifer Coughlin



Jennifer Coughlin
Partner, Mullen Coughlin LLC

Jennifer Coughlin is a founding partner of Mullen Coughlin. She focuses her practice on providing organizations of all sizes and from every industry sector in first-party breach response and third-party privacy defense legal services. In the context of incident response, Ms. Coughlin has counseled thousands of clients in investigating and responding to an event compromising information and systems security, working closely with client resources, third-party forensic consultants, and law enforcement to identify the nature and scope of a compromise. Ms. Coughlin relies on her knowledge of state, federal, and international laws, as well as industry-specific guidances and standards to assist organizations in identifying and complying with legal obligations to disclose the incident to certain audiences and provide certain services to impacted populations.

Regarding regulatory counsel, Ms. Coughlin has represented numerous organizations, including healthcare centers, healthcare treatment providers, financial institutions, hospitality providers, online and brick-and-mortar retailers, hotels, and other professional services providers in inquiries by regulators, including state attorneys general, state insurance departments, state health departments, the Federal Trade Commission, the U.S. Department of Health and Human Services, and the Office for Civil Rights.

Ms. Coughlin also provides regulatory compliance services and incident response planning services to organizations. She has assisted hundreds of organizations from all industry sectors in policy/procedure preparation, incident response planning, tabletop exercises, and staff training, custom-tailored by the organization's data privacy risks and applicable industry-specific laws.

Jennifer Coughlin

Recent Evolution of Ransomware and Business Email Compromise Events*

An interesting evolution in ransomware and business email compromise events occurred over the past few years. While ransomware was the most common type of cyber event experienced in 2019, 2020, and 2021, business email compromise – many of which involve wire fraud – climbed to the top rank as of the second quarter of 2022. Cyber claims continue to evolve. Implementation of cybersecurity best practices is resulting in organizations being better risks for cyber insurers, and better positioned to defend, detect, and contain cyberattacks.

The past.

Ransomware can be catastrophic, with victims facing crippling cessation of system operations and data access. There is an immediate need to become operational, and minimize business interruption and the potential exfiltration of sensitive data. Reputational damage can be entity-threatening. Organizations can choose to not pay ransoms depending on their ability to recover operations and data access from backups or alternative sources. Not all businesses are equipped with healthy backups or other data recovery options, though. Additionally, many ransomware attacks now include exfiltration of sensitive data. This was not the case in the past. Exfiltrated data creates an additional pressure point to force a ransom payment. Entities face the choice of paying hush money to the threat actor – payment in exchange for the promise of deletion of the exfiltrated sensitive data, a promise that the organization will never be able to verify. Difficult choices. Note that making such a payment does not alleviate the need to comply with disclosure laws.

The table below provides the number of ransomware events handled by Mullen Coughlin from 2019 to 2021, the number and percentage of clients that paid ransoms, the average ransom demand, the average ransom payment, and the median ransom payment. While the volume of ransomware matters, average ransom demand, and median ransom payment increased during these years, the percentage of victims that paid the ransom and average ransom payment DECREASED.

Year	Total Number of Ransomware Matters	Payment of Ransom	Average Demand	Average Payment	Median Payment
2019	581	137 (24%)	\$526,153	\$283,752	\$78,520
2020	959	291 (30%)	\$1,916,194	\$579,539	\$165,000
2021	1,128	297 (27%)	\$2,127,838	\$485,439	\$210,052

Although a business email compromise does not interrupt systems or business like ransomware, it can nevertheless be devastating. Such an event may result in lost revenue due to the misdirection of payments meant for the victim organization (or a victim's business partner or client) to a fraudster's bank account, reputational damage due to the use of the account to send phishing emails to client contacts and others, third party liability risks, and the unauthorized acquisition and/or access to data contained within the compromised email account(s).

The table below provides the number of business email compromise events handled by Mullen Coughlin from 2019 to 2021 and the number of matters in which the fraudulent transfer or misdirection of funds occurred. During these years, the number of business email compromises overall – and the number that involved fraudulently wired monies – increased, while the amount of monies fraudulently transferred stayed relatively flat.

Year	Number of Business Email Compromise Matters (Total)	Number of Business Email Compromise Matters (with Wire Fraud)	Average Amount of Fraudulently Wired Money
2019	546	63 (12%)	\$301,585
2020	959	291 (30%)	\$319,413
2021	987	345 (35%)	\$312,720

The present.

2022 has been very different from 2019, 2020, and 2021. As of the second quarter of 2022, business email compromise is now the most common type of cyber event facing Mullen Coughlin clients, with the percentage of matters involving wire fraud and the average amount of fraudulently wired money being similar to 2019-2022.

Year	Number of Business Email Compromise Matters (Total)	Number of Business Email Compromise Matters (with Wire Fraud)	Average Amount of Fraudulently Wired Money
2019	437	142 (32%)	\$319,856

The volume of ransomware matters, percentage of victims paying the ransom, average payment, and median payment have all declined while the average demand continues its upward climb from years prior.

Year	Total Number of Ransomware Matters	Payment of Ransom	Average Demand	Average Payment	Median Payment
2022	360	49 (14%)	\$2,319,868	\$381,318	\$178,500

The future.

Organizations are taking more seriously now than ever before the impact a cyberattack can have on its business, and focusing more efforts on improving cyber hygiene. These improvements include the purchase of cyber insurance, which provides an organization with immediate access to expert resources needed to quickly, efficiently, and in a cost-effective manner, investigate and respond to data privacy events. Appropriate insurance provides resources on how to be more secure, and better detect and defend against cyberattacks. As more organizations continue to implement cybersecurity best practices, it gives hope that businesses of all sizes, from all sectors, and from around the globe will be able to withstand the anticipated increase in threat actor activity and cybercrime to come.

* The information contained in this chapter is current as of the date of publication, and the information, including cited statistics, is subject to change post-publication. The author makes no representation or warranty regarding the accuracy of such information after the time of publication.

Chapter Five

Combat Ransomware through Resilient Backups

By Jeff Reichard



Jeff Reichard

Vice President, Public Sector & Compliance Strategy, Veeam Software

Jeff Reichard is Vice President, Public Sector & Compliance Strategy at Veeam, where he drives strategic product and go-to-market engagement with public sector and enterprise customers. Jeff has 25 years of experience in data protection/availability, business continuity, and regulatory compliance solutions. At Veeam, he works with partners, customers and industry analysts to evangelize Veeam's vision for modern data protection at key events worldwide.



Jeff Reichard

Combat Ransomware through Resilient Backups

Ransomware is pervasive in 2022, with organizations of all types and sizes routinely attacked to devastating effect. Specifically, in a large 2022 survey of 4,500 organizations worldwide, Veeam found that 76% had been hit by at least one ransomware attack in 2021. Most organizations were attacked between one and three times, and some were hit 6+ times in 2021 alone.

Organizations must plan not for if, but when they suffer a successful attack. We can't always prevent a cyberattack, but Veeam customers have found that they can take steps to guarantee successful recovery when an attack occurs.

Back up everything, because all workloads get hit

In Veeam ransomware research published in May 2022, we asked 1,000 organizations targeted by ransomware in 2021 where their data was infected by ransomware: in the data center, in remote offices, or in cloud compute resources. There was no significant difference in data encryption rates between these three locations, with over 50% of security professionals saying that each location had data encrypted.

In other words, we can't assume that only laptops, or only data center resources, will be affected. Cloud data is attacked at the same rate as data anywhere else. So it's critical to have backups of all data that your organization relies upon – whether on-premises or in the cloud.

Protect those backups

Cybercriminals routinely attempt to encrypt or delete an organization's backups as part of a ransomware attack. In the same ransomware research mentioned above, Veeam asked: "Did the threat actor attempt to modify/delete backup repositories as part of the ransomware attack?" The overwhelming

majority, 94%, had their backup data attacked.

To weather that attack, organizations must create resilient backup copies that cannot be destroyed by an adversary — even one who has acquired administrative credentials. Fortunately, there are many ways to achieve this, from simply removing backup tapes from the library to using immutable object storage in the public-cloud or on-premises. But it is critical that you have one or more layers of protection in place.

One simple way to remember this is the 3-2-1 rule. To be secure, we should have 3 copies of all important data – one production copy and two backups. Those should be on at least 2 media types for safety, and 1 copy should be offsite. One or more of these backup copies must be resilient against attacks from an adversary who has acquired administrative credentials.

Automate backup and recovery testing

In our 2022 ransomware study, Veeam also asked respondents how much data they were able to recover after an attack. While answers varied, the global average was 64%. This figure includes respondents who paid a ransom to get their data back. Paying a ransom is no guarantee of recovery. It is critical to test backup and recovery success in an automated manner. It's not enough to look at a backup log, see success, and declare victory. Testing must include the ability to remediate any malware in backup copies. It must be automated, because manual processes inevitably break down or become outdated. And as the statistics above indicate, after a successful attack is not the time to discover that one-third or more of your data is lost forever. While successful cyber defense requires many layers, secure backup is the critical last line of defense.

Coming back to the topic of cyber insurance, backups give incredible leverage when negotiating a ransom payment and they are often required by insurers when completing an application. To learn more about Veeam's research on this topic, please look at the following resources: [Data Protection Trends 2022](#) and [Ransomware Trends 2022](#)

Chapter Six

Reduce Your Cyber Liability with Preemptive Email Security

By Shalabh Mohan



Shalabh Mohan

Head of Product, Cloudflare Area 1

With a career spanning 20+ years fighting bad guys online, Shalabh is responsible for product, go-to-market & customer success for Cloudflare Area 1. With extensive prior experience across security, enterprise, and cloud infrastructure companies, Shalabh and his teams have taken products from conception all the way to large scale businesses; and in the process have consistently helped make the Internet a safer place. An alumnus of Stanford University and University of Texas at Austin, Shalabh is a holder of 5 patents and can claim to know something about enterprise infrastructure, security and complex price modeling. An avid sports nut and a bigger fantasy football fanatic, Shalabh is known to get severely distracted by travel, books, movies and food.



Shalabh Mohan

Reduce Your Cyber Liability with Preemptive Email Security

Ransomware, a type of malware that blocks access to data or systems typically by encrypting it, continues to plague organizations. “Famous” variants like Revil spread rapidly, crippling organizations and leaving billions of dollars in damages for expensive recovery costs.

Disturbingly, other ransomware like Ryuk have zeroed in on specific industries, like hospitals and healthcare organizations¹. Using targeted phishing emails, attackers behind Ryuk hope these organizations may be more likely to pay Ryuk’s substantially higher ransom when there are literally lives at stake.

In fact, ransomware is expected to cost its victims more around \$265 billion (USD) annually by 2031, with a new attack (on a consumer or business) every 2 seconds². The damage due to recovering from downtime can also cost much more than the ransom payout itself.

Increasing ransomware attacks require security leaders to look beyond endpoint solutions and response strategies, with an end-to-end strategy that includes detecting and stopping ransomware before they reach end users.

Enter preemptive [email security](#) to defend against ransomware attacks.

While attackers have traditionally favored remote code execution (RCE) exploits as the ransomware delivery mechanism, when RCEs are unavailable, attackers make phishing emails the “go-to” mechanism.

Attackers often rely on the factor of human mistakes, and cognitive biases can reliably be exploited through phishing and social engineering. This is cy-

clical in nature, with threat actors switching between various tactics and **organizations must be prepared to defend against all types of cyberattacks.**

Ransomware phishing emails typically deliver a first stage loader, such as Trickbot, a banking Trojan increasingly used to spread ransomware. By using commodity malware such as stagers, ransomware threat actors do not risk losing as much if their attacks are caught — all they stand to lose is some phishing infrastructure (e.g., lookalike email domains) and the fact that they are targeting a particular organization.

The time it takes for ransomware to be deployed on a network has exponentially decreased over time. Several years ago, it took several months for ransomware to be deployed. Today, it takes hours or less from the moment an end user or a network is compromised.

By the time most organizations realize they have been compromised, attackers have already exfiltrated large amounts of data to hold hostage. With ransomware’s increased targeting and sophistication, an organization’s best chance of surviving a ransomware attack is to prevent it from reaching the organization in the first place.

Adept at detecting first stage loaders before ransomware can be deployed, the Cloudflare Area 1 service offers comprehensive email security against sophisticated phishing attacks. Area 1’s preemptive threat signals and campaign indexing can discover malicious infrastructure in the earliest stages of attack creation. Area 1 leverages small pattern analytics to detect even the most targeted threats, without needing to rely on large volume samples. Area 1 also uniquely uses deep payload scanning to detect ransomware hidden in links within attachments, nested links, or archives, even if domain fronting tactics are used.

Taking a preemptive approach to email security can stop phishing emails from ever reaching your inbox — and, ultimately — stop ransomware from reach-

ing your inbox. The ability to correctly identify phishing attempts is an important part of cybersecurity awareness training, and will complement any cyber insurance policy.

To identify which phishing threats and ransomware loaders are evading your current defenses, request a complimentary [Phishing Risk Assessment](#) from Cloudflare Area 1.

¹“Alert (AA20-302A) - Ransomware Activity Targeting the Healthcare and Public Health Sector.” Cybersecurity & Infrastructure Security Agency (CISA.gov), 28 October 2020, last revised 2 November 2022. <https://www.cisa.gov/uscert/ncas/alerts/aa20-302a>

² “Ransomware Costs Expected to Reach \$265 Billion by 2031.” Cybercrime Magazine, 2 June 2022. <https://securityintelligence.com/news/ransomware-costs-expected-265-billion-2031/>

Chapter Seven

An Investor's Perspective on the Future of Cyber Insurance

By Victoria Cheng



Victoria Cheng

Partner, PruVen Capital

Victoria is a Partner at PruVen Capital. She specializes in FinTech/InsurTech, Healthcare IT, and Enterprise SaaS. Previously, she served as Director of Venture Investing at Citi Ventures, where she was an early investor in companies such as Plaid, Braze, DataRobot, Immuta, Bluevine, Hopper, and TMP. There, she also launched and co-led the Citi Impact Fund for Citi Ventures, a \$200MM program created in joint partnership with Citi SPRINT and GPA, to invest into sustainability, infrastructure (housing, transportation, healthcare), workforce development, and financial capability. This team also drove the development of a Seed Program to invest in very early stage startups founded by women and minorities to increase the pipeline of diverse founders. Previously, Victoria was a Senior Associate at Core Innovation Capital, a FinTech venture capital firm investing in the democratization of financial services, where she was involved with investments in TIO Networks, Ripple, and Oportun. Prior to Core, she consulted for Foundation Capital, and worked with NYC Seed to build its Seed Start Media Accelerator. Her experience before venture investing, includes working with startup, NimbleTV, private equity investing, and investment banking focused on power & utilities.

Victoria graduated with honors from Columbia Business School, and received her undergraduate degree from Georgetown University, where she graduated magna cum laude. She is a Kauffman Fellow and an InSITE Fellow. Victoria is passionate about diversity and inclusion. She serves on the advisory board of Money2020's Rise Up program and runs the Women's Fundraising Cohort Program for Kauffman, which works to drive more LP capital to experienced diverse VC managers.



Victoria Cheng

An Investor's Perspective on the Future of Cyber Insurance

At PruVen, we get excited about 1) **insurance markets** that are both growing and where incumbents do not have a competitive advantage over startups, and 2) **startups** that have underwriting and risk management that is highly differentiated from traditional carriers.

1) Attractiveness of the Cyber Insurance Market for Startups: Cyber insurance is one of the largest growing categories in commercial insurance. It is also an area of insurance where new players can begin on an almost even playing field with incumbent carriers. The following three characteristics exemplify this:

- Demand is outpacing supply and the market is experiencing hyper-growth. We look for markets where environmental factors support rapid growth. The market demand for cyber insurance policies is robust and growing rapidly. The increased business reliance across all industries and size of businesses on the internet has created more exposure to cyber risk. At the same time, regulations around data privacy have put greater onus on companies to manage their cyber exposure. The recent prevalence of ransomware (and the media coverage of attacks) has raised awareness of the cybersecurity threats to small and medium-sized businesses. As a result of these factors, we expect that the number of companies that purchase cyber will increase and the individual policies will also increase in size over time.

- Historical claims data is not a moat because risk changes quickly and continuously, and new technologies are more suitable for addressing this risk. Cyber insurance, unlike many other P&C segments, is constantly evolving and claims data ten years ago is not necessarily indicative of the risks ten years from now. Being on the forefront of cyberse-

curity technology is a competitive advantage in this sector. Furthermore, being able to provide best in class cyber monitoring, protection, and mitigation to customers is beneficial for ongoing risk assessment and exposure management.

- Historically, the experience of purchasing a cyber policy is poor. Purchasing cyber insurance is often cumbersome, manual, time-consuming, and does not always accurately reflect the inherent risk in the businesses being covered. The typical process consists of a lengthy (often paper-based) questionnaire of over a hundred questions and a period of up to 90 days. Startups can leverage technology to make the experience more digital and more automated.

2) Actuarial to Actual: We see a movement in insurance away from pricing risk based on historical aggregate cohort calculations toward writing policies that are specifically tailored for the policyholder with an ever-evolving perspective of the future. We refer to this trend as the shift from Actuarial to Actual underwriting and risk management. This new underwriting approach enables a carrier to be more proactive, personalized, forward-looking, and accurate in their risk assessment. We look for specific startups that are building with this thesis in mind.

In cyber, we see this reflected in Cowbell. The company monitors the digital footprints of 30M small businesses in America for their cyber risk exposure as the cyber risk in the market changes. Based on the team's deep expertise in cybersecurity, they change the pricing, coverage, or underwriting criteria to effectively reflect that exposure to the broader population. Then on a granular level, they continuously monitor the security posture of each of their policyholders and provide proactive notifications about emerging threats in their specific situations along with the steps to take to mitigate cybersecurity exposures and protect their businesses.

We look forward to seeing the evolution of cyber insurance and to supporting Cowbell as they continue building a category-defining company in cyber insurance.

Chapter Eight

Cyber Insurance: How Policyholders Can Mitigate Their Own Cyber Risk

By Isabelle Dumont



Isabelle Dumont

SVP Marketing and Technology Partners, Cowbell

Isabelle leads market engagement at Cowbell, including cyber insurance go-to-market, partnerships with cybersecurity providers, and all marketing functions. Isabelle brings 13 years of cybersecurity experience built at Palo Alto Networks where she launched industry-specific initiatives, at BlueTalon, a data-centric security leader acquired by Microsoft, and at Lacework, a cloud security unicorn. Isabelle has a track record of driving high growth for innovative businesses in emerging markets by connecting technologies to business benefits. She also held senior positions at Oracle and holds a master in artificial intelligence from Ecole Centrale in France.



Isabelle Dumont

Cyber Insurance: How Policyholders Can Mitigate Their Own Cyber Risk

By 2030, cyber insurance in-force premiums in the U.S. [will total \\$100 billion](#), according to a Cowbell estimate. As more companies opt-in for cyber insurance, organizations are ramping up their security controls to get the best coverage and the lowest premiums. We're seeing policyholders proactively improving their cybersecurity posture to best protect themselves from cyberattacks.

It's imperative that businesses address security issues before even applying for cyber insurance. This is a matter of insurability. Take it from us: we're highly unlikely to agree to knowingly insure a company and take on risk when there are gaps in that company's security protocols because it is more likely to need to pay out their coverage during the term of the policy.

This process also empowers security teams to push for the extra funding they may need to resolve outstanding vulnerabilities and reinforce the urgency behind addressing the issues. With external consequences and potential impacts on the business' bottom line at stake, leadership teams are facing the unappealing prospect of being uninsured against cyberattacks. This increases the priority of resolving vulnerabilities within the organization.

The most common issues we see that need to be addressed include not having incident response or backup plans and lacking basic security training for employees. Here are a few tips businesses can use to become better prepared for cyberattacks and more insurable:

- Create and communicate incident response plans
- Test backups
- Train employees to recognize security threats
- Patch existing issues
- Maintain an inventory of digital assets

Some companies also offer assessments for potential policyholders to identify the issues that should be resolved before applying for coverage and benefits to customers who have implemented preventative measures.

When selecting a cyber insurance provider, an organization should be mindful of finding one that offers not only third-party liability coverage, which historically has been the only type of coverage available, but also first-party loss and first-party expense coverage to help the business recover from an attack. Cyber policies should also come bundled with the basic resources and advice that insureds need to continuously evaluate and manage their cyber exposures: cyber risk assessment, cyber management resources, risk engineering and more.


Once insured, organizations need to continue to be mindful of new and emerging risks and show continual security improvements—by doing so, they will open themselves up to more coverage options from their insurers.


They must also remain cognizant of the state of their own digital footprint, as any change to this, including implementing different workplace collaboration tools or hiring a new remote employee, can result in new security vulnerabilities and risks. However, if an organization demonstrates a continued commitment to improving its risk profile, they may have better options when it comes time to renew the policy.

It's important for businesses to recognize that risk is constantly changing. The risks that cyber insurance covers, and the cyber insurance industry itself, are also expanding as a result. This is where [adaptive cyber insurance](#) comes into play. The field is growing at a rapid pace, with demand at an all-time high and organizations realizing that coverage is no longer optional. In the face of an evolving threat, Cowbell is offering [continuous risk assessment](#) and [continuous underwriting](#) to help organizations get ahead of future threats and exposures, which companies should use to their advantage to ensure they remain protected moving forward.



 Headquarters:
6800 Koll Center Pkwy, Suite 250, Pleasanton, CA 94566

 Main Line:
+1 (833) 633-8666

 Website:
cowbell.insure