ConversationalGeek®

Conversational Cyber Insurance

By Joseph Brunsman (Founder, Brunsman Advisory Group)

In this book, you will learn:

- What is and isn't covered within a cyber insurance policy
- The technologies you need to have in place to help meet cyber insurance requirements
- How identity security and PAM helps to meet cyber insurance requirements

3rd Edition

Sponsored by

Delinea

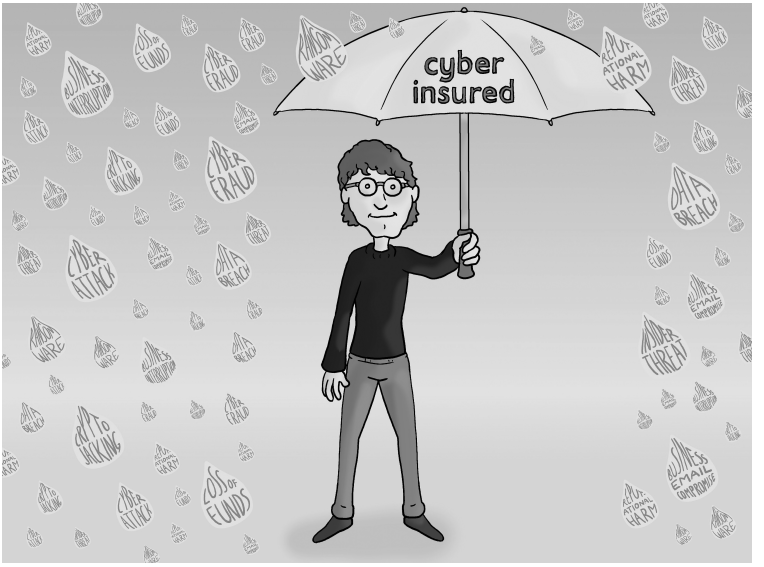
Sponsored by Delinea

Delinea is a leading provider of Privileged Access Management (PAM) solutions for the modern, hybrid enterprise. The Delinea Platform seamlessly extends PAM by providing authorization for all identities, controlling access to an organization's most critical hybrid cloud infrastructure and sensitive data to help reduce risk, ensure compliance, and simplify security. Delinea removes complexity and defines the boundaries of access for thousands of customers worldwide. Our customers range from small businesses to the world's largest financial institutions, intelligence agencies, and critical infrastructure companies.

For more details visit
delinea.com

Conversational Cyber Insurance
(3rd Edition)

By Joseph Brunsman



ConversationalGeek®

Conversational Cyber Insurance

Published by Conversational Geek® Inc.

www.conversationalgeek.com

Trademarks

Warning and Disclaimer

Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at ConversationalGeek.com

Publisher Acknowledgments

All of the folks responsible for the creation of this guide:

Author:	Joseph Brunsman
Project/Copy Editor:	Ian Whiteling
Content Reviewer(s):	Jayson Gehri
	Rob Sawyer

Note from the Author

The world of cyber insurance is still in an evolving state; in short, insurance companies are still trying to figure this thing out. And that means there's little-to-no chance that those within an organization responsible for cyber insurance and its impact on cybersecurity strategy and execution can clearly understand exactly how a policy can and can't help you.

In this eBook, I'm going to simplify cyber insurance down to its fundamentals, cover the process of assessing cyber insurance requirements, spend some time discussing the common exclusions you may encounter with a cyber insurance policy, and then explain how technologies supporting Identity Security can help either attain a policy or help protect an organization so that, should you be attacked, you'll (hopefully) never need to make a claim.

Joseph Brunsman

The “Conversational” Method

We have two objectives when we create a “Conversational” book: First, to make sure it’s written in a conversational tone so that it’s fun and easy to read. Second, to make sure you, the reader, can immediately take what you read and include it into your own conversations (personal or business-focused) with confidence.

These books are meant to increase your understanding of the subject. Terminology, conceptual ideas, trends in the market, and even fringe subject matter are brought together to ensure you can engage your customer, team, co-worker, friend, and even the know-it-all Best Buy geek on a level playing field.

“Geek in the Mirror” Boxes

We infuse humor into our books through both cartoons and light banter from the author. When you see one of these boxes it’s the author stepping outside the dialog to speak directly to you. It might be an anecdote, it might be a personal experience or gut reaction and analysis, it might just be a sarcastic quip, but these “geek in the mirror” boxes are not to be skipped.

Greetings. Within these boxes I can share just about anything on the subject at hand.

Read ’em!

How Cybersecurity and Cyber Insurance are Intertwined

"Here! You're going to need all this!"

In Wodruff-Sawyer's Cyber Insurance Trends report, 100% of cyber insurance underwriters believe cyber risk will increase over the next 12 months.[1] As the former CEO of IBM once stated, "We believe that data is the phenomenon of our time. It is the world's new natural resource. It is the new basis of

[1] Wodruff-Sawyer, *Looking Ahead: Cyber Insurance Trends for 2024* (2024)

competitive advantage, and it is transforming every profession and industry. If all of this is true – even inevitable – then cybercrime, by definition, is the greatest threat to every profession, every industry, every company in the world."[2]

And organizations around the world are experiencing this threat en masse. With cybercrime stats like 95% of organizations experiencing at least one ransomware attack in the last year[3], the number of phishing attacks rising by 58%[4], and cybercrime costs expected to rise to $24 trillion by 2027[5], it's evident that cybercrime is, indeed, the greatest threat – with little evidence to suggest that it will do anything but increase in the coming years.

So, what can your business do in light of such persistent and dire threats? There's an old joke about two hikers sitting in a tent, when a bear comes charging towards them. The first man immediately starts running away, while the second man starts putting on his shoes. The man running turns around and yells, "Your shoes won't help you outrun the bear!" To which the second man replies, "I don't have to outrun the bear, I just need to outrun you!"

Much like the above story, there is very little, if anything, that your business can do offensively. Therefore, your only option is to maximize defense. Within this realm, you have two primary categories: cybersecurity and cyber insurance. While these two ideas were traditionally seen as two separate topics, you'll see

---

[2] "IBM's CEO On Hackers: 'Cyber Crime Is The Greatest Threat To Every Company In The World'", forbes.com, accessed June 23, 2024

[3] Extrahop, *Global Cyber Confidence Index* (2024)

[4] Zscaler, *ThreatLabz 2024 Phishing Report* (2024)

[5] Munich Re, *Cyber insurance: Risks and Trends* (2023)

below that they are becoming more intertwined and interdependent every year.

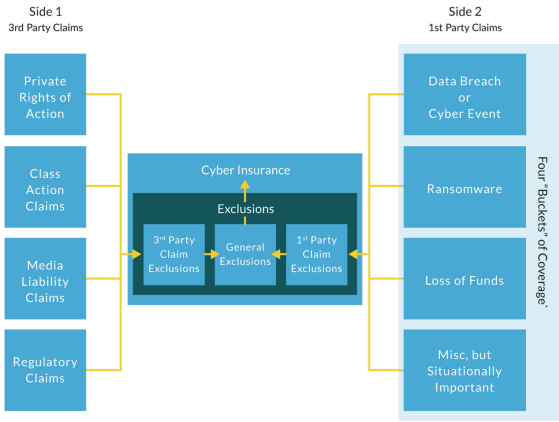
Let's Talk About Cyber Insurance

The vetting and purchase of appropriate cyber insurance can appear to be an overwhelming task for even the most accomplished executive. Understanding that "cyber insurance" is not a legal term, nor even a standard insurance industry term, this conundrum can seem even more onerous. However, with a little background knowledge, a bit of preparation, and some organization, this experience can be made much simpler.

What is "Cyber Insurance?"

There are hundreds, if not thousands, of different cyber policies from insurance companies worldwide. Each insurer attempts to provide their own unique offering to gain an advantage over their competition. This can range from greater sub-limits of coverage to industry specific coverage options. Regardless of the length of a cyber policy, the wording used, or the number of attachments included within a quote page, they can be easily organized to provide a better coverage assessment for your business.

Each cyber policy quote can be fundamentally broken down into two "Sides," four "Buckets," and a series of "Exclusions" – issues explicitly not covered by the policy.



Breaking down the fundamentals of cyber policies

Side One – Third-Party Claims

Following some type of cyber event, it is possible that some type of claim, or lawsuit, may be brought against your business. This could include clients or vendors who believe they've suffered damages from identity theft or loss of your services. In addition, your business could face a demand from payment card companies if payment card information was stolen and used for fraudulent purchases under your PCI DSS (Payment Card Industry Data Security Standards) agreement. Or perhaps, you could face a Media Liability claim where a plaintiff alleges copyright infringement.

Finally, there is always the specter of regulatory inquiries, fines, and penalties. It is worth noting that these are typically insurable under a cyber insurance policy. However, they often contain a caveat that fines and penalties are generally allowed, "where insurable by law." What regulatory cybersecurity regimes your business may fall under is difficult to determine with any certainty as laws and precedents evolve so quickly in this area.

To illustrate this point, take a recent case where the Federal Trade Commission (FTC) brought action against a U.S.-based car dealership. You may be surprised to learn that the FTC, an organization ostensibly founded to enforce civil U.S. antitrust law, would concern itself with enforcing cybersecurity standards. In the case at hand, it was alleged that a car dealership installed Peer-to-Peer file-sharing software on their corporate network.[6]

Not only did the FTC argue that this violated Section 5(a) of the FTC Act, a law passed in 1914, but they also alleged that the car dealership had violated a specific provision within the Gramm-Leach-Bliley Act (GLBA).[7] It should be noted that the GLBA was a law enacted in 1999 that required financial institutions to safeguard specific consumer information. In total, the car dealership agreed to a consent order requiring nearly six pages of mandatory cybersecurity and administrative controls specifying constant vigilance and periodic assessments over the course of the next 20 years[7]. The costs to comply with such orders are also generally uninsurable.

How does the FTC – and most other government regulatory entities – judge the cybersecurity of businesses? On their website they note that they use the NIST Cybersecurity Framework (NIST CSF).[8] Depending on your circumstances, this could turn any specific control from a "nice to have" into a potential "legal requirement." While a quick look at the NIST

---

[6] FTC Finalizes Settlements with Businesses that Exposed Consumers Sensitive Information by Installing Peer-to-Peer File-Sharing Software on Corporate Computer Systems (Federal Trade Commission)

[7] Franklin's Budget Car Sales, Inc., also d/b/a Franklin Toyota/Scion, In the Matter of (Federal Trade Commission)

[8] The NIST Cybersecurity Framework and the FTC (Federal Trade Commission)

CSF can be daunting, you should know that certain controls may satisfy multiple criteria.

Imagine your business is assessing the following Identity Management and Access Control subcategories:

- PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes
- PR.AC-3: Remote access is managed
- PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
- PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)
- PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions

In all the above, an appropriate Identity Security solution – specifically with Privileged Access Management (PAM) functionality – may fulfill some or all of each subcategory.

In much the same way, an appropriate antivirus and anti-malware solution could meet NSIT CSF subcategories DE.CM-4: Malicious code is detected, and DE.CM-5: Unauthorized mobile code is detected.

Your business could be subject to multiple and conflicting cybersecurity laws. Make sure you're working with legal counsel to determine what rules you need to follow.

While third-party claims from individuals tend to be less common in the cyber insurance arena, it is worth researching what exposure you may have and how cyber insurance may cover those losses.

Side Two – First-Party Claims

This is what businesses most commonly think of as cyber insurance. Despite your best efforts at defense, something bad happened internally and you are looking for legal guidance and reimbursement for your losses. Coverage for these "bad" events can be broken down into four "buckets" of potential coverage.

Bucket One – Data Breach or Cyber Event: A Data Breach is generally defined as both access and acquisition of personal information. While the exact definition of a breach will vary based upon the type of information you hold and the industry you operate in, affected parties are generally afforded breach notification and credit monitoring. If your assigned cyber attorney determines that the breach is large enough after consulting with the assigned forensic team, you may also be assigned a public relations expert, a call center to field the legion on inbound call from angry affected clients, and a crisis management professional to assist your business.

Likewise, your business may fall victim to a Business Email Compromise (BEC) event or some other type of cyber intrusion. In circumstances such as those, having forensics experts assess your system, and legal counsel to assist you with the myriad of regulatory and contractual issues your business may face is certainly useful.

If either of these two events were to occur, you would be looking for the following fundamental coverage elements: Attorney, Forensics, Business Interruption Reimbursement for any downtime your business faces, and Data Restoration costs.

Bucket Two – Ransomware: Unfortunately, basic ransomware events do not need further explanation due to the frequency. When a ransomware event occurs, your business will be looking for an attorney, ransom negotiator, ransom payment, data restoration, business interruption, and forensics.

Bucket Three – Loss of Funds: In this area, your business needs to pay particular attention because how terms are defined varies wildly across policy forms. Policy features can range from absolutely necessary to being suspect in their usefulness. Typically, businesses are worried about two potential scenarios. First, their own business may be conned into transferring their own firm funds. Second, their system may be used by a hacker to trick the business's clients into transferring money owed to the business, somewhere else. Regardless of what you may assume a coverage means, that should be checked by reading the policy's definitions in light of your own business's potential loss scenarios.

Certain policies have rules that must be evidenced before your business is reimbursed for a loss of funds. Make sure you're following the rules before a loss occurs!

Bucket Four – Miscellaneous but Situationally Important: This category could contain any number of situationally useful items. Often seen items in this category include: Reputational Harm, Crypto-Jacking, First or Third Bodily Injury or Property Damage, Voluntary Shutdown Coverage, and Dependent Business Interruption Reimbursement. Make sure you read the definitions of these coverages before you purchase a policy because they could be crucially important for your unique business, or potentially useless.

It should be kept in mind that in some circumstances, the above buckets of coverage may overlap each other in ways entirely dependent on the fact pattern of the cyber event.

What You Should Consider Before Applying for Cyber Insurance

The days where businesses could purchase a cyber insurance policy with a brief questionnaire are gone. As losses mount, cyber insurers are taking a harder look at the cybersecurity posture of businesses.

Generally, the application process can fall into three categories:

1. The business fills out an extensive questionnaire concerning the technical, administrative, and physical safeguards they have implemented.

2. The business fills out a basic questionnaire but is mostly judged on an external vulnerability scan to determine their insurability.

3. The business is subject to an extensive questionnaire as well as external, and potentially internal, vulnerability scanning.

Though every cyber insurer is going to have their own requirements, it's clear that the majority of insurers are now viewing the following controls as a likely mandate before insuring medium to large sized businesses:

- Multifactor Authentication (MFA)
- Endpoint Detection and Response (EDR)
- Identity Security
- Incident Response Planning and Testing

- Multiple Backups – multiple backups, with offline and immutable backups being viewed more favorably.
- Email Filtering and Web Security
- Patch Management and Vulnerability Management
- Security Awareness Training and Phishing Testing
- End of Life Systems Replacement – meaning unsupported hardware/software is replaced.
- Supply Chain Risk Management and Mitigation.

While the head of IT and Cybersecurity will certainly be busy with completing the insurance application, cyber insurance should not be viewed as solely within the purview of their department. Cyber events can impact every area of a business and each part of business may have its own "nightmare scenario." Attempts to silo the responsibility for procuring cyber insurance with one person can very easily lead to important coverages being completely overlooked. For this reason, it is advisable to have the head of each business function first meet to determine what cyber risks they want to insure for.

For example, the CEO may be worried about Reputational Harm coverage, the Director of IT might be concerned about the cost to replace hardware. The CFO may be concerned about cybercrime losses, or the head of HR may view a data breach as their worst-case scenario. These concerns should be directly addressed with your insurance broker during the application process.

You will always know the risks to your business better than any insurance broker. Make sure your concerns are known!

After The Quote

Now that you broadly understand what could be contained within a cyber insurance policy, as well as what unique concerns your business has, it is time to put them together. Once you have your quote(s) in hand, re-visit each concern to determine how, if at all, that concern is insured. In certain circumstances, cyber insurance may only insure a loss to a certain amount, or perhaps not at all. It is also possible that certain rules must be evidenced before your business is reimbursed. Most commonly this last mandate is seen in the "Loss of Funds" category.

While your cyber insurer may not necessarily mandate a particular control, the business case for implementation of that control may now be more apparent. If you cannot ensure for a specific loss to an acceptable degree, various controls could be used as a hedge against such an issue.

Renewing Cyber Insurance

As the cyber insurance market continues to tighten, and insurers demand more specific controls, the renewal process will continue to become a tougher prospect. Increasingly we are seeing cyber insurance companies demand specific controls before they will issue a quote. Depending on the insurer, they may not issue a quote unless those controls are previously implemented – in which case you may never know – or they may demand specific controls be implemented before your quote can be bound and the policy issued.

Exacerbating this problem is the fact that insurers are constantly reassessing specific industries, the size of businesses within those industries, and the controls they possess. Even without a cyber event, and through no fault of your own, your business may receive a letter 60 to 90 days (or less) before renewal where your cyber insurer states that they will no longer offer you a cyber insurance policy. This means your business may be subject to a host of additional cybersecurity requirements that must be implemented in short order.

The larger your business, the more complicated and time-intensive this process can become. As implementation deadlines become more compressed, it is more likely that sub-optimal solutions are implemented, and that execution mistakes will occur. This is yet another reason why it is preferable for businesses to consistently evaluate their cybersecurity posture in light of industry best practices and evolving threats.

No matter what cyber insurance provider your business currently works with, or may work with in the future, they are all broadly asking the same question: "Whether on-prem, or in the cloud, how hard would it be for a bad actor to access this company's data?" As cyber insurers increasingly place security demands upon their customers, this is where planning ahead can pay serious dividends for your business.

Besides being a good idea, implementing additional cybersecurity controls can have a material impact on your premium.

Assessing Cybersecurity Requirements for Cyber Insurance

For IT Directors, CISOs, and similar positions, contemplating the changing cyber insurance requirement landscape leaves quite the conundrum on how to best position their business in the future. As threats, insurance company requirements, and insurance policies change, a seemingly infinite number of possible avenues to increase security seem apparent. While these choices can seem overwhelming, decision makers should remember that there are ultimately three categories to be constantly assessed and evaluated: *people*, *processes*, and *technology*. It is necessary for all three to act in harmony for maximum security to be obtained. After all, the best technology in the world can't overcome a determined end-user, and no end-user is savvy enough to overcome all technical threats on their own.

When it comes to *people* and *processes*, education, and standardization are of utmost importance. People should be trained consistently on current and evolving threats. This could include phishing scams, social engineering, good password hygiene, and personal safeguards when working from home.

Processes are generally much easier to create, but more difficult to manage. On the technical side, this could include disaster recovery, business continuity, and backup recovery plans. When threats, or potential threats, are discovered, this may also include incident response plans that vary based upon the general risk presented.

Standardized processes for the personnel side are often overlooked, but are crucial – according to underwriters, with half of them believing companies should focus on *improving processes and procedures* as the top risk mitigation strategy[1]. Your business might create a standardized process for how and where employees should report suspect communications for further review. It may also include specific requirements for the transfer of money from your business to minimize social engineering losses. Second person review, prearranged callback

numbers, passcodes, and other potential requirements as dictated by your insurance policy or bank specific security measures, should be created and rigorously enforced.

Unfortunately, as humans, we get tired, distracted, or disinterested in security. When it comes to cybersecurity, humans need to be right every time, but the bad guys only need to get lucky once. This is where robust technological solutions can add crucial support to your people and processes; ideally making them a redundant security feature as opposed to a primary point of potential failure.

How AI May Impact Cybersecurity and Cyber Insurance

The use of AI has been seen on both sides of the cybersecurity battlefront – with threat groups building out AI-based platforms to enable more credible, sophisticated, and successful attacks; and with cybersecurity vendors heavily relying on AI to help detect attacks and respond to them quickly.

According to Wodruff-Sawyer:

"Inherently, AI won't change cyber risk. But it may exacerbate the severity of a problem when it arises."

As cyber insurers continue to evaluate both the nature and state of cyber readiness by their insureds, as well as the use of AI in successful attacks resulting in claims, I suspect we'll see a greater requirement on the part of underwriters to see specific use of AI in multiple aspects of cyber defenses as a means of fending off the risk posed by threat-used AI technologies.

Those organizations who can demonstrate employing AI as part of their cybersecurity defenses may see some benefits as it relates to their obtaining of cyber insurance, including:

- Risk Reduction – Using AI for proactive threat detection and response reduces the likelihood of breaches, making the organization a lower-risk client for insurers and a more likely candidate to receive a policy.
- Premium Discounts – Insurers may offer premium discounts or more favorable terms to organizations that demonstrate robust AI-driven cybersecurity measures.
- Enhanced Coverage Options – Improved security posture through AI may qualify organizations for broader or more customized coverage options.

Equally, those organization not implementing and utilizing AI may see the exact opposite results, making AI critical to lowering cost and improving insurance coverage.

The Role of Identity Security in Cyber Insurance

Obtaining an adequate cyber insurance policy should not be seen as a cure-all solution for business leaders. As the market grapples with increasing losses, half of cyber insurers expect underwriting scrutiny to increase to limit their own exposure[1]. Furthermore, governmental bodies at various levels are making efforts to address this pressing issue.

While reviewing the terms and conditions of an insurance policy may not be a source of great pleasure for business leaders, it is a vital responsibility as cyber risks and cyber policies are subject to constant changes. Relying solely on a broker or agent for advice on policy modifications and their implications could prove hazardous. Unless extraordinary circumstances exist, agents and brokers are generally not obligated to provide advice to insureds regarding the sufficiency or suitability of their policy.[9] Even later pleading that you relied on an agent or broker who claimed specialized knowledge or expertise in this domain may not persuade certain courts in the event of a coverage dispute.[10]

Ultimately, it is your responsibility to determine whether your current cyber insurance policy already encompasses any, or all, of the following exclusions and how they might impact your business.

It is important to note that policy language is evolving rapidly, with one or more exclusions potentially already *being included*, *or being added* shortly before renewal, are *causing specific*

---

[9] Jerry, Robert, *Understanding Insurance Law*, Carolina Academic Press, 2018, page 208

[10] Jerry, Robert, *Understanding Insurance Law*, Carolina Academic Press, 2018, page 210

controls to be implemented within a similar timeframe to remove or modify an exclusion.

Included in these specific security controls is the need for Identity Security (which includes PAM functionality), detects identity-related threats and manages access and entitlements both on-premises and in the cloud, restricting and governing access to elevated privileges that would otherwise provide threat actors unsanctioned access to your organization's sensitive systems, applications, and data.

A great example of how identity security controls are becoming a de facto standard in cybersecurity implementations goes beyond just cyber insurance. Take the New York State Department of Financial Services' *Cybersecurity Requirements for Financial Services Companies*, better known as 23NYCRR500.

Section 500.7 (entitled *Access Privileges*) contains a requirement stating that all Class A financial companies must "monitor privileged access, implement PAM and commonly-used password blocking"– and have this in place by May 1, 2025.

By ensuring only approved identities can access privileged accounts or obtain elevated privileges for approved activities, organizations reduce the ability for threat actors to take advantage of the elevated privileges and entitlements needed to carry out malicious actions. Additionally, should a claim be made, insurers require the insured organization to *prove* the controls were in place at the time of the incident. Having Identity Security controls in place means also having an ability to establish whether privileged credentials were used during a

cyberattack, on what systems, and potentially what actions were taken – all necessary to help substantiate the claim.

Let's look at some of the specific cyber insurance exclusions that may exist in either a current or future policy and see how identity security can be used to help mitigate either the risk of a successful attack or the organization risk introduced by the exclusion.

OFAC Exclusions

It is highly likely that every cyber insurance policy in the United States includes a seemingly innocuous notice regarding the U.S. Department of Treasury's Office of Foreign Asset Control (OFAC). However, what many business leaders may not be aware of is how the most recent OFAC "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments"[11] intersects with their cyber insurance and the disastrous implications it could have for their businesses.

According to OFAC, "Facilitating a ransomware payment that is demanded as a result of malicious cyber activities may enable criminals and adversaries with a sanctions nexus to profit and advance their illicit aims... U.S. persons are generally prohibited from engaging in transactions, directly or indirectly, with individuals or entities on OFAC's [sanctions lists]."

It goes without saying that businesses are unfortunately unable to determine which strain of ransomware infiltrates their systems and whether that payment leads back to a sanctioned entity, thereby preventing payment. So, what happens if a ransom is paid in good faith, only for it to be later discovered that the payment benefited a sanctioned entity?

---

[11] U.S. Department of the Treasury, *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* (2020)

OFAC has addressed this possibility, stating, "OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if they did not know or have reason to know that they were engaging in a transaction with a person prohibited under sanctions laws and regulations administered by OFAC." In other words, ignorance is not an excuse, and penalties can still be imposed.

This naturally raises the question of whether any civil penalties could be covered by a cyber insurance policy. The short answer is: It depends.[12] The insurability of such penalties depends on a multitude of factors, none of which you would likely want to delve into after experiencing a ransom event while also facing federal sanctions.

While OFAC's notice does include a provision that allows for a potential waiver, the implications are not particularly encouraging. The notice states, "Ransomware payments benefit illicit actors and can undermine the national security and foreign policy objectives of the United States. For this reason, license applications involving ransomware payments demanded as a result of malicious cyber-enabled activities will be reviewed by OFAC on a case-by-case basis with a presumption of denial."

According to a legal expert, submitting a request to OFAC for a waiver could take up to six months for basic transactions and even up to a year for more complex matters.[13] In the interim, your cyber insurer could freeze any ransom payments. Clearly,

---

[12] Abraham, Kenneth S., The Insurability of Civil Fines and Penalties (April 13, 2023). forthcoming, 58 Tort Trial and Insurance Practice Law Journal, Virginia Public Law and Legal Theory Research Paper No. 2023-33

[13] "Filing a Request for Interpretive Guidance from OFAC", ofaclawyer.net, accessed June 23, 2023

this timeframe offers little assistance during a rapidly unfolding – and potentially very expensive – cyber event.

Imagine a scenario where every document held by your business is going to be released unless a ransom is paid. However, your cyber insurer believes that a sanctioned entity may be involved and refuses to release payment until OFAC gives their permission. The potential long term legal liabilities alone could be catastrophic.

How Identity Security Helps Address the OFAC Exclusions

The bottom line is, if your attacker is on the OFAC list, and a ransom is being solicited, you can't pay it. So, the only proactive response here is to minimize the risk of such an attack being successful. In other words, *take away the threat actors' ability to hold your organization for ransom*.

In every ransomware attack, the threat actor needs access to multiple systems and data sets – something that requires privileged access to both connect to and to encrypt. By implementing identity security controls including securing privileged accounts in an enterprise vault, minimizing standing privileges at both the local, domain, and cloud levels, and continually monitoring access to identity use and behavior, you minimize – if not completely remove – a threat actor's access to sensitive systems and data, preventing unauthorized access, movement, and encryption of critical data.

Ransomware Coinsurance and Sub-limits

It has come to light that at least one insurer has completely prohibited ransomware payments.[14] Ironically, shortly after implementing this strict measure, a segment of their own

---

[14] "Insurer AXA to Stop Paying for Ransomware Crime Payments in France", insurancejournal.com, accessed June 23, 2023

business was hit by ransomware.[15] While this extreme approach appears to be currently limited to a single insurer, others are taking steps to sub-limit their ransomware coverage. Essentially, this means that while the policy may provide full coverage for other types of cyber events up to the policy limits, ransomware could be treated differently for your business.

Outlined below are three common methods insurers are using to reduce their exposure to ransomware risks while simultaneously increasing the burden on your business. Depending on the insurer, they may employ one or more of the following methods:

1. Lowering the available coverage for all costs associated with ransomware.
2. Imposing limitations on the coverage for ransomware costs unless the business can provide evidence of implementing specific controls.
3. Requiring the business to pay both the deductible or retention and an additional percentage of the overall cost as "coinsurance" following a ransomware event. It is important to understand that a deductible or retention represents the amount of risk your business is willing to accept. Thus, introducing a coinsurance requirement through a discreet endorsement buried deep within the policy significantly increases the financial burden your business could face.

---

[15] "Ransomware Attack Reported at Insurance Giant AXA One Week After It Changes Cyber Insurance Policies in France", CPO Magazine, accessed June 23, 2023

How Identity Security Helps Address Ransomware Coinsurance and Sublimits

This brings us back to the crucial need for implementing appropriate defense mechanisms to ideally prevent a ransomware attack entirely, thereby also avoiding complications with insufficient sub-limited coverage and unforeseen coinsurance requirements.

In addition to restricting access to local and domain privileged accounts in an enterprise vault, PAM – as part of a comprehensive identity security strategy – can specifically also require multi-factor authentication and password rotation. This makes it much harder for threat actors to exploit even a reportedly "compromised" privileged account because the password has already changed and there's no ability for the threat actor to provide the required additional authentication factors.

Legacy Hardware and Software Exclusions

It is increasingly common for certain cyber insurance policies to exclude coverage for cyber events involving unsupported systems. These systems can encompass applications, operating systems, firmware, software, and hardware. One significant challenge faced by IT professionals is justifying the replacement of legacy systems when the existing solution is still operational.

Similarly, certain businesses may find it economically infeasible to replace network elements. For instance, some manufacturers rely on multi-million-dollar equipment connected to their network that has not been supported for decades. Or the equipment runs on custom software within antiquated operating systems. On the other hand, other businesses may possess custom software that functions perfectly well but would incur exorbitant costs to replace.

In cases like these, the expense of replacing the legacy hardware or software may far exceed the costs associated with addressing a cyber event by orders of magnitude. Consequently, it would be prudent to consider whether reducing your attack surface or, at the very least, mitigating the access and impact of internal threats.

How PAM Helps Address Legacy Hardware and Software Exclusions

The primary concern here on the part of insurers is that old hardware and software may include vulnerabilities no longer being addressed by the manufacturer. These vulnerabilities could be exploited to provide access. But, if an exploit were to be used, the best-case scenario for the threat actor is to gain elevated privileges on the legacy system. They still need to logically move laterally within the network and gain access to a more privileged account that gives them access to more than just an old server running even older software.

Identity security controls can limit access to systems, restrict privileges on those systems, manage remote session access, and monitor for misuse of privileged credentials, resulting in the isolation of legacy systems and elimination of lateral movement potential by malicious actors. This safeguards other systems and data from their potential harm.

Critical Vulnerability Exclusions

Those who have spent countless hours dealing with "Patch Tuesday" know that patching vulnerabilities and updating systems is often far from seamless. It seems that there's always a patch that ends up breaking something else, turning Patch Tuesdays into Patch Early Wednesday Mornings or even Patch Saturdays. The same headaches are compounded by off-cycle critical security and vulnerability updates.

Adding to the complexity, some businesses, such as accounting firms, may operate on highly seasonal schedules where statutory deadlines effectively prevent any changes to their systems. Even non-seasonal businesses may face critical deadlines throughout the year that temporarily halt patching, much to the frustration of the IT department.

Unpatched systems have naturally led to significant claim payouts for cyber insurance companies, which could have been avoided altogether. For cyber insurers, paying out claims for unpatched vulnerabilities is akin to replacing a vehicle under an auto insurance policy when the car was left running, unlocked, in a high-crime neighborhood.

Moreover, malicious actors are aware of the patching cadence even at responsible companies, and they are increasingly attempting to exploit this potential vulnerability. According to one report, 55% of reported vulnerabilities were exploited within seven days of disclosure.[16]

In response, cyber insurers have started incorporating exclusions in their coverage for unpatched critical vulnerabilities. These exclusions often state that vulnerabilities meeting a certain base score within the Common Vulnerability Scoring System (CVSS) must be remedied within a specified number of calendar days. As an example, an illustrative policy might exclude coverage if a vulnerability scored 8 or higher on the CVSS and the patch was not deployed within 14 days of its release.

The actual threshold for vulnerability score and the required remediation timeframe will depend on the specific language of your policy. However, given current trends in exploit activity, it is highly likely that both the vulnerability score threshold and

---

[16] Rapid7, *2024 Attack Intelligence Report* (2024)

the remediation timeframe for coverage will decrease in the foreseeable future.

To mitigate the potential impact of this exclusion in your current or future policy, there are several tools at your disposal. Foremost a vulnerability and patch management system should help your organization keep on top of such a requirement.

How Identity Security Helps Address Critical Vulnerability Exclusions

Similar to exploits of legacy hardware and software, critical vulnerabilities not addressed by organizations within the allotted time can provide comparably elevated access to the exploited system only.

Managing and monitoring privileged accounts, standing privileges, as well as human and machine user access and elevation policies are critical for limiting the damage caused by a threat actor post-exploit, as they can be used to restrict where and when privileged access can be used. Identity security solutions offer an additional layer of security by providing just-in-time (JIT) and just-enough (JEP) privileged access which reduces the value of the compromised accounts even if they did have elevated privileges. These solutions ensure that unauthorized access and elevation of user and machine identities are blocked, meaning that even if a threat actor was to exploit a system with accounts that should have had elevated privileges, those accounts would have no value to the threat actor as they cannot be accessed without going through a PAM solution.

Zero-Day Exclusions

Perhaps the most concerning exclusion in the cyber insurance market is the inclusion of exclusions for claims related to zero-day exploits in certain policies. These exclusions encompass

zero-day exploits (which represent 43% of all exploited vulnerabilities) arising from applications, operating systems, software, hardware, and more. It can be argued that coverage for unforeseen, unavoidable, and unpredictable losses is one of the main reasons businesses invest in cyber insurance. These factors also explain why cyber insurers are eager to avoid providing coverage for such events.

How Identity Security Helps Address Zero-Day Exclusions

From an insurer's perspective, there is little difference between a claim involving a zero-day exploit and one involving an exploit of a vulnerability that wasn't patched. In either case, the insurer isn't going to foot the bill for it.

There's also little difference from an identity security perspective. Both zero-day and known (but unpatched) critical vulnerabilities leave the organization open to attack, but each requires privileged access beyond the initially compromised system. But with identity security solutions in place, where can the threat actor go? Unless the compromised system has valuable data, the threat actor needs to move laterally within the network – something identity security eliminates completely by restricting access to the privileged accounts and minimizing standing privileges that could facilitate such movement.

Widespread Event and Limited Impact Exclusions

Recent widespread events – such as the Log4j vulnerability and supply chain attacks – have raised significant concerns in the cyber insurance industry. These events have the potential to impact a vast number of policyholders simultaneously, leading to massive losses that could jeopardize the financial stability of insurance companies. As a result, certain insurers are starting to introduce Widespread Event Exclusions in their policies.

While the specific wording may differ among insurers, these widespread event endorsements can potentially exclude coverage for many of the previously mentioned exclusions, including known vulnerabilities, software supply chain exploits, zero-day vulnerabilities, and other broadly categorized "All Other Widespread Events."

However, the devil lies in the details. The definition of a "Widespread Event" varies depending on the policy language, often leaving room for interpretation, and potentially leading to costly and lengthy legal disputes for resolution.

Here are some concerning provisions found in the policy forms of a prominent cyber insurer:

- Coverage limitations and a coinsurance requirement for losses resulting from known vulnerabilities with a Common Vulnerability Scoring System (CVSS) score of 8.0 or higher, regardless of whether a patch has been issued.
- Sub-limited coverage at varying levels, potentially as low as 10% of the original insurance limits, with a coinsurance requirement of up to 25% for any known vulnerability, regardless of its published severity, if it has not been patched within specified timeframes ranging from forty-six days to over a year.
- Coverage limitations and a coinsurance requirement for vulnerabilities introduced into a business's computer system through software developed by a trusted software developer, distributed to multiple customers, and considered trusted due to a digital certificate.
- Coverage limitations and a coinsurance requirement for zero-day exploits that later receive a CVSS score of 8.0 or higher.

- Coverage limitations and a coinsurance requirement for potentially any other widespread event that is not categorized as a supply chain exploit, zero-day vulnerability, or known vulnerability.

In all of the scenarios mentioned above, mitigating the impact of the event becomes crucial for the survival of the business. Depending on the method of intrusion, you may have no initial defense and, potentially, no coverage under your cyber insurance policy.

How Identity Security Helps Address Widespread Event Exclusions

The issue at hand is that these kinds of attacks result in so many victim organizations that to cover resulting claims would leave the insurer too exposed and unable to cover all claims. It should be noted that the issue isn't the initial method of attack (although that is the crux of how they're defining this exclusion); it's the result of such an attack, with countless organizations exposed by data exfiltration, extortion, data held for ransom, and businesses unable to operate.

While no one knows what the next widespread attack will be that results in elevated access to countless thousands of organizations, we do know that identity security will serve as an effective defense against a threat actor's ability to gain a foothold in a victim network and cause significant damage. Identity security protects against a threat actor's ability to:

- Take over privileged accounts
- Establish local persistence
- Move laterally to other systems and into the cloud

- Access and control directory services,
- Manipulate and/or exfiltrate data
- Wreak havoc on organization productivity

All these threats are effectively eliminated by minimizing or eliminating standing privileges, storing critical privileged credentials in an enterprise vault, enforcing JIT and JEP best practices, and monitoring privileged access. With identity security controls in place, an organization can be assured that even if a supply chain or widespread attack is initially successful, the threat actor will not have the ability to cause extensive damage.

Reputational Harm Sub-limits

In the past, it was not uncommon for businesses, including large ones, to have coverage for "reputational harm" that reimbursed for the loss of revenue and reputation following a cyber event. However, this type of coverage is now largely absent from the marketplace or significantly diminished, making it practically useless for all but the smallest businesses.

A recent study by the Ponemon Institute highlighted "Lost Business" as the second-largest form of loss following a cyber event, closely trailing incident response costs. Previous studies have shown that a significant percentage of clients, ranging from four to seven percent, can leave a business after a cyber event. In response to such losses, approximately 60% of businesses increased their prices following a data breach. Given current economic realities, losing clients and subsequently increasing costs would not bode well for a company.

A well-known business maxim is that it is easier and cheaper to retain existing clients than to acquire new ones. With cyber insurance no longer covering lost client revenue, containing a

cyber event becomes even more crucial. A recent study on data breach class action claims revealed two important findings: large companies incurred an average cost of $1.4 million to defend a data breach case, with an average settlement of $2.6 million, and the likelihood of litigation increased as the number of breached records grew.[17]

These claim costs alone are concerning, but when added to the expenses of a cyber event, they have the potential to exceed policy limits and require the victimized company to pay significant out-of-pocket expenses. Even after a case is settled, higher incident costs can result in increased difficulties and costs in obtaining cyber insurance for at least five years, if it is offered at all. The impact of disclosure and court proceedings on a company's reputation is unknown, but it is unlikely to be positive. Businesses should strive to retain clients and avoid costly litigation whenever possible.

How Identity Security Helps Address Reputational Harm

We're getting down to repercussions of attacks, rather than the technical acts taken within the attack itself. Identity security's place is to *stop* threat actions. So, this one is more a case of using identity security controls to help stop an attack that would otherwise have reputational repercussions using the features already mentioned.

Act of War Exclusions

New nation-state attack exclusions in cyber insurance policies are becoming a cause for concern among business leaders. While traditional insurance policies have long excluded coverage for acts of terrorism and war, the inclusion or

---

[17] Kesan, Jay & Zhang, Linfeng. (2021). When Is A Cyber Incident Likely to Be Litigated and How Much Will It Cost? An Empirical Study, Connecticut Insurance Law Journal.

exclusion of coverage for cyberwarfare has been a more recent challenge. Notable examples include the roughly $10 billion fallout from the NotPetya virus, where major insurers grappled with coverage decisions, resulting in high-profile disputes that took years to settle.[18]

In response to such massive challenges, Lloyd's of London, a prominent international insurance and reinsurance market, issued new guidance in March 2023. The guidance mandates that cyber insurance policies issued through Lloyd's must include an exclusion for losses arising from state-sponsored cyber-attacks.[19] However, the specific wording of the exclusion has not been provided, leaving some ambiguity.

One of the most significant concerns for business leaders regarding this exclusion is the issue of attribution. Attributing a cyber event to a specific individual or state, or proving otherwise, can be a costly and time-consuming process, and in some cases, it may be nearly impossible. The intelligence required for attribution may be classified by governments, leading to disputed validity. This was evident in the case of the NotPetya events, where official attribution was based on a four-sentence press release from the White House Press Secretary.[20]

Regardless of the wording of the policy, it is inevitable that disputes will arise where coverage for nation-state attacks is being contested. Even if your business is successful in litigation, you will still face uncovered losses until the dispute is resolved, which could take years. Until case law catches up with the

---

[18] " Oreo Giant Mondelez Settles NotPetya 'Act of War' Insurance Suit", darkreading.com, accessed June 23, 2023

[19] Lloyds, *State backed cyber-attack exclusions Market Bulletin* (2022)

[20] https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/

interpretation of policy wording, business leaders can only do their best to avoid or minimize the impact of potential nation-state attacks.

How Identity Security Helps Address Acts of War

What makes these types of attacks so dangerous is that nation-states are funding these attacks, giving threat actors essentially unlimited resources to find the most sophisticated and effective ways to compromise and take over a victim network.

Identity security's use of JIT and JEP, governance over which users can access privileged accounts, where privileged accounts can be used, and MFA enforcement at access or elevation stands toe-to-toe with the most advanced threat groups, rendering their access and ability to maliciously act upon a victim network null and void.

In short, no privilege, no access, no successful attack… all thanks to securing identity.

Business leaders should be aware that the cyber insurance market is undergoing rapid and significant changes, and these changes are likely to continue in the foreseeable future. It's important to understand that even if your current cyber insurance policy does not have any of the exclusions mentioned earlier, it doesn't guarantee that you are fully protected. A single cyber event could lead to your business being deemed non-renewable, forcing you to seek coverage in the open market where these exclusions are becoming more prevalent. Additionally, your insurer may introduce these exclusions during your policy renewal, even if you haven't filed any cyber insurance claims.

The days of relying solely on cyber insurance without adequately investing in cybersecurity measures is no longer a viable approach. It is crucial for businesses to allocate appropriate resources to strengthen their cybersecurity

posture, which includes implementing suitable solutions like a Privileged Access Management (PAM) system. By proactively investing in cybersecurity, businesses can mitigate the impact of common exclusions that may already exist in their cyber insurance policies or are likely to be implemented in the future.

The Big Takeaways

Keeping in mind all the above information, those in charge are increasingly looking towards technologies that fulfill the following requirements:

- The ability to monitor, track, and limit both human and non-human privileged activities as much as possible.
- Proactively detect identity-related threats like account takeovers through password stuffing, MFA bombing, and brute force.
- Creating a "least privilege strategy" to grant only as much access as is needed for functions to be performed, leveraging just-in-time (JIT) and just-enough privileges (JEP) to ensure human and machine identities that would otherwise be at risk have no standing privilege.
- Password management automation that forces robust requirements as dictated by the business.
- Auditing and tracking the usage of privileged activities.
- Identity validation with MFA enforcement from initial log-in through every step of access.
- The capacity to monitor identity behavior to dynamically adjust privileged access and security challenges as dictated by risk profile or anomalous/abnormal behavior.
- Accomplishing the above while creating the least amount of friction for users and the least amount of disruption for the business; ideally with a lower cost of ownership, and on a single platform.

Most, if not all, of the above solutions can be implemented with an appropriate Privileged Access Management (PAM) Solution. As was alluded to previously, it is increasingly becoming common for cyber insurers to demand that a robust PAM solution be implemented as a prerequisite to renewing, or obtaining, a cyber insurance policy.

Whether your business is explicitly required to implement PAM by your insurer at this moment is somewhat irrelevant. For the foreseeable future, cyber policy premiums will continue to grow, new exclusions will be added, and coverages will shrink. In tandem, cyber threats are forecasted to only increase.

Finally, any cyber event experienced by your business will likely require increased controls to facilitate a renewal. So, no matter what the avenue of adoption, increased cybersecurity makes sense.

Review the Privileged Access Management controls needed for cyber insurance

FREE Cyber Insurance Readiness Checklist from Delinea

This sample cyber insurance checklist guides you through the top questions most insurance companies ask when you apply for cyber insurance.

Delinea

Download now:
delinea.com/resources/cyber-insurance-checklist

Quickly become conversational about cyber insurance.

With thousands of different insurance policies available from different brokers worldwide, it can be hard to know which one best suits the needs of your business. This book will help guide you through how the cyber insurance industry works, the requirements you need to understand to obtain coverage, and how security solutions assist in meeting requirements while protecting the organization.

About Joseph Brunsman

Joe is a graduate of New Mexico Military Institute and the United States Naval Academy where he obtained a degree in Systems Engineering. He is the author of several books and various publications on the topic of cyber insurance and is the founder of the nationwide insurance brokerage, Brunsman Advisory Group, LLC.

ConversationalGeek®

For more content on topics geeks love visit

conversationalgeek.com