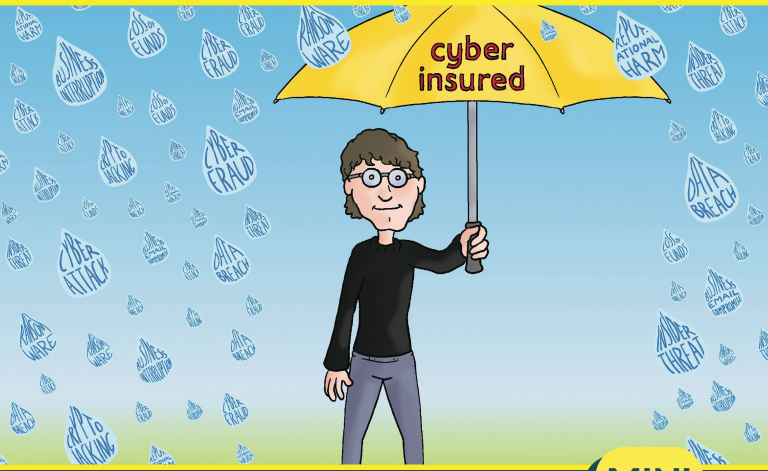
ConversationalGeek

Conversational Cyber Insurance

Joseph Brunsman (Cyber Insurance Expert)



MINI Edition

Learn about:

- How to understand 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

Sponsored by

Delinea

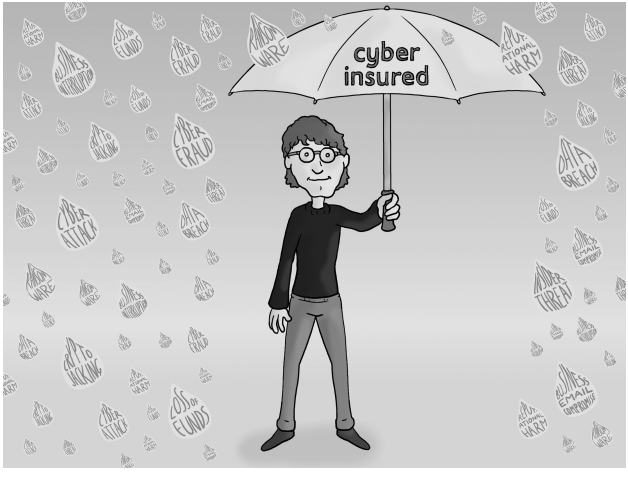
Sponsored by Delinea

Delinea is a leading provider of privileged access management (PAM) solutions that make security seamless for the modern, hybrid enterprise. Our solutions empower organizations to secure critical data, devices, code, and cloud infrastructure to help reduce risk, ensure compliance, and simplify security. Delinea removes complexity and defines the boundaries of access for thousands of customers worldwide, including over half of the Fortune 100. 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 (Mini Edition)

by Joseph Brunsman



ConversationalGeek®

Conversational Cyber Insurance (Mini Edition)

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 www.ConversationalGeek.com.

Publisher Acknowledgments

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

Author:	Joseph Brunsman
Project and Copy Editor:	Pete Roythorne
Content Reviewer:	Jayson Gehri

The “Conversational” Method

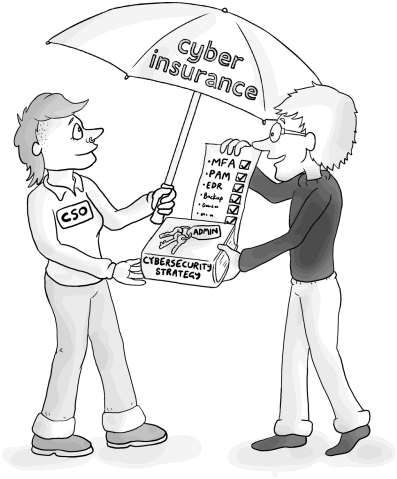
We have two objectives when we create a “Conversational” book. First, to make sure it’s written in a conversational tone so that it’s fun and easy to read. Second, to make sure you, the reader, can immediately take what you read and include it into your own conversations (personal or business-focused)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

“Geek in the Mirror” Boxes

We infuse humor and insight 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.

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 PWC's 25th Annual Global CEO Survey, respondents listed cyber risks as their top threat to growth.[1] As the former CEO of IBM once stated,

---

[1] www.pwc.com/gx/en/ceo-agenda/ceosurvey/2022.html

“We believe that data is the phenomenon of our time. It is the world’s new natural resource. It is the new basis of 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]

Meanwhile, the headlines do not inspire confidence. Forbes recently posed the question, “Why Are We Losing the Cyber War?” They followed with another article replete with depressing statistics, declaring there were “50% more attack attempts per week on corporate networks globally in calendar year 2021 compared with 2020,” and, “$43 billion stolen through Business Email Compromise since 2016, reports FBI.”[3]

---

[2] IBM's CEO On Hackers: ‘Cyber Crime Is The Greatest Threat To Every Company In The World’ (Forbes)

[3] Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know (Forbes)

When a headline from six years ago stated, "America is Losing the Cyber War"[4] it should come as no surprise that The New York Times recently released an article entitled, "How the United States Lost to Hackers."[5]

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:

---

[4] Cyber Wars: How the U.S. Stacks Up Against its Digital Adversaries (US News)

[5] How the US Lost to Hackers (New York Times)

cybersecurity and cyber insurance. While these two ideas were traditionally seen as two separate topics, you'll see below that they are becoming more intertwined and interdependent every year.

Let's Talk About Cyber Insurance

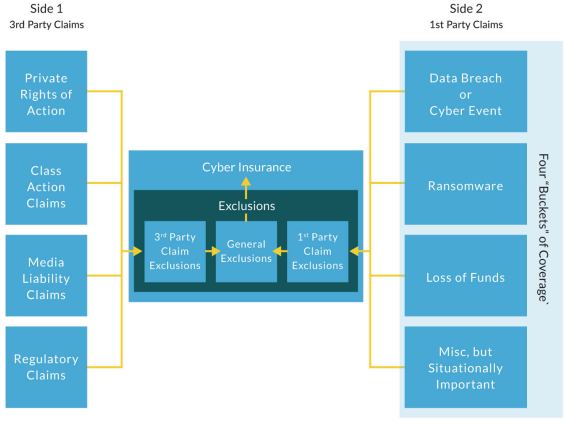
The vetting and purchase of appropriate cyber insurance can appear to be an overwhelming task for even the most accomplished executive. Understanding that "cyber insurance" is not a legal term, nor even a standard insurance industry term, this conundrum can seem even more onerous. However, with a little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

---

[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)

requiring nearly six pages of mandatory cybersecurity and administrative controls specifying constant vigilance and periodic assessments over the course of the next 20 years.[8] 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).[9] 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 CSF can be daunting, you should know that certain controls may satisfy multiple criteria.

---

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

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

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 Privileged Access Management (PAM) solution 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.

Considerations and Requirements before applying for cyber insurance:

The days where businesses could purchase a cyber insurance policy with a brief questionnaire are quickly coming to end. 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)
- Privileged Access Management
- 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 Tests

- 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 consistent and evolving threats. This could include phishing scams, social engineering tricks, password protection requirements, 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, nonetheless. 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.

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 accounts as much as possible.
- Creating a “least privilege strategy” to grant only as much access as is needed for functions to be performed.
- Password management automation that forces robust requirements as dictated by the business.
- Auditing and tracking the usage of privileged accounts.
- Identity validation with MFA from initial log-in through every step of access.
- The capacity to monitor user 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

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 and the requirements you need to understand.

About Joseph Brunsman

Joe is a graduate of the United States Naval Academy with a Bachelor's degree in Systems Engineering, and the Carey School of Law with a Master's in Cybersecurity Law. He is the founder of the insurance brokerage The Brunsman Advisory Group, where he handles the cyber insurance needs of organizations nationwide.