CYVATAR.AI

8 EPIC CYBERSECURITY FAILS

BY CRAIG GOODWIN & COREY WHITE
CO-FOUNDERS OF CYVATAR

TABLE OF CONTENTS

INTRODUCING THE

UNF**KING CYBERSECURITY COMIC SERIES

By Cyvatar

This is not your average eBook! We created an eight-part comic series for each chapter's theme. Sit back, relax, and enjoy a bit of comic relief. And if you get a laugh, feel free to take a screenshot and share it on social media—tag us @cyvatar!

Comic strip illustrated by Matt Bradshaw for Cyvatar.
Here are the dramatis personae:

Super Security Company Rep

CEO

CTO

CISO

CFO

CRO

Super Security Company Rep #2

Cyber Staffer

Customer

Super MSSP Rep

Post-Breach CEO

Post-Breach CISO

TLDR

THIS BOOK IN A NUTSHELL

The cybersecurity industry was founded to prevent people and organizations from getting breached, but in the three decades since the first reported computer virus the hacks haven't stopped. If anything, they've grown more visible and virulent.

Three major security concerns—cyber attacks, data fraud, and information theft—made the World Economic Forum's top 10 list of long-term risks in 2020. All three were considered either most likely to occur, most impactful should they occur, or most concerning for doing business globally.[1]

Under such circumstances, it's hardly surprising that eight and a half *billion* people were affected by cyber attacks last year—more than the number of people currently walking around on the planet—which means some percentage of the population was hit more than once.

Clearly, the industry has failed to keep pace with the adaptability of today's cyber criminals, causing us to purchase time and again the latest security tools in an attempt to keep our sensitive and confidential information safe.

But the hacks keep coming.

Could it be that the security industry is, in fact, NOT designed to stop breaches?

Our goal in writing this book is to help you cut through the marketing noise and bring rationality and accountability into your buy process to make your organization more secure. We're here to show you that you don't have to fall victim to the industry's vicious cycle of selling you products that are more or less designed to fail: You can meet your business and cybersecurity requirements without sacrificing one for the other.

But before we go any further, let's make sure we're all on the same page. You'll hear us talk a lot about the importance of business outcomes and business value, so let's take a moment to think about what that means.

WHAT DRIVES YOUR BUSINESS?

Business drivers vary by organization, but there are some universal themes:

- To decrease business risk
- To reduce the complexity of IT investments
- To support faster sales cycles and improve business velocity
- To achieve better compliance
- To improve customer retention, loyalty, and advocacy
- To prevent data and information breaches

This book addresses ways to enlist cybersecurity to ensure the success of your business goals.

[1] World Economic Forum. "*The Global Risks Report 2020*." January 15, 2020.

WE BELIEVE IN THE POWER OF TRANSFORMATIONAL CHANGE TO CREATE UNPRECEDENTED BUSINESS VALUE.

We know change is painful. We know it's hard to recognize when change is imperative—because we've been there. We've experienced every one of the epic fails in this book, we've made mistakes, we've lost value, we've been duped by vendor false promises. We've been in the trenches and believe passionately in building better alternatives.

We believe that if you challenge yourself, your organization, and your providers to make the changes necessary to ensure you achieve successful business outcomes, you'll regain your agency and boost your security confidence.

This book walks through each security fail in detail and offers guidance to help you achieve measurable time to value every step of the way. It wraps with a six-point checklist and a plan to help you move forward with a successful cyber strategy, regardless of where you are in your security journey.

We believe in the power of transformational change to create unprecedented business value. This book will help you achieve it.

- Corey + Craig

CHAPTER

1

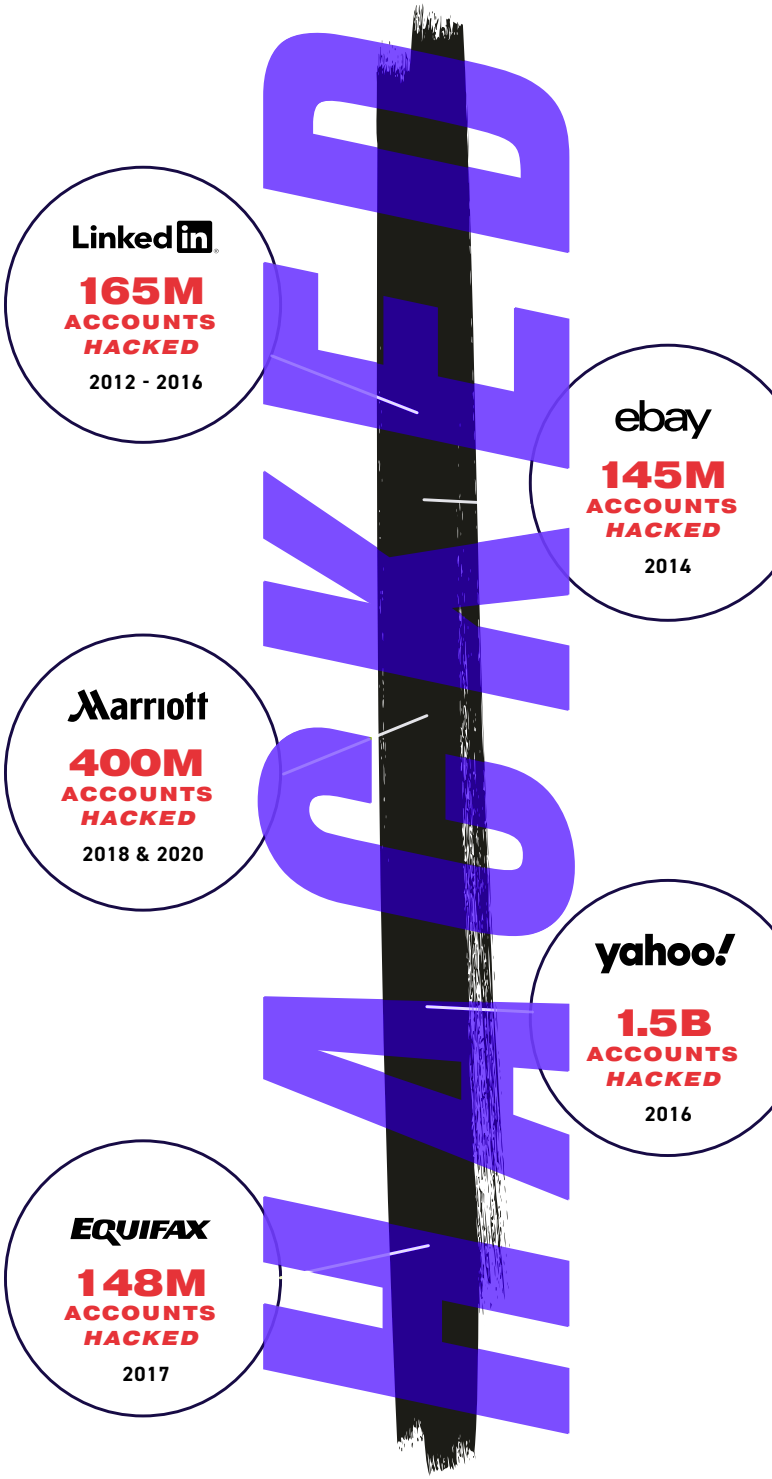
THE SECURITY INDUSTRY *LIES*

UNF**KING CYBERSECURITY by CYVATAR.AI

Okay. So maybe "lies" is a strong term, but the cybersecurity industry was founded on the idea of preventing people and organizations from getting hacked.

Yet for more than 30 years,[2] cyber attacks have grown. Hacks that made the headlines include 1998's sniffer attacks on U.S. military targets by three teenagers, 2012's Stuxnet worm that attacked a nuclear research facility in Iran, and 2017's WannaCry ransomware attack that infected some 200,000 devices in nearly 150 countries.

And let's not pretend the companies we trust with our personally identifiable information (PII) fared any better at keeping our individual details safe. As you can see from the snapshot on the right, billions of customer accounts were exposed to cyber criminals in less than a decade across just five organizations.



ICYMI: **8.5 BILLION people were affected by cyber attacks last year. That's more than every person drawing breath on the planet, which means some percentage of the population was hit more than once. It also means organizations large *and* small were impacted.**

In other words, the security industry has failed—spectacularly failed—to keep pace with the adaptability of today's cyber criminals, resulting in a tag-team approach of persuasion and pressure on business leaders like you to stoke your fears of being breached. The industry uses fear, uncertainty, and doubt (FUD) to goad you into purchasing, time and again, the latest security tools in an attempt to keep your sensitive and confidential information safe.

But buying from fear of attack doesn't make your organization any safer—in fact, it's likely to introduce more risk—and drive more profit for an industry that consistently fails to protect you.

LESSON #1

The perception of risk, seen through the lens of fear, interferes with our ability to make good decisions.

[2] Since1989 and the first reported computer virus, created by Robert Morris.

SOPHOS, ONE OF THE SECURITY COMPANIES RESPONSIBLE FOR PROTECTING THE U.K.'S NHS FROM WANNACRY, FAILED TO KEEP 70,000 NHS DEVICES SAFE—STILL, ITS SHARES JUMPED 8% IN THE DAYS FOLLOWING THE ATTACK.

Security solutions that rely on FUD to sell more product play on your fear of a cyber incident and cloud your ability to make rational purchases based on your business goals rather than vendor promises. It's a strategy rooted in adversarial or wartime propaganda—cyber war took its cue from traditional war—without realizing that digital warfare is a whole new animal.

Hackers aren't soldiers in a bunker. Not all hackers are even bad actors. But taking an old-school view of cyber war delivers a false sense of security, security based on fear that makes it difficult—if not impossible—for you to dispassionately evaluate the risks that genuinely threaten your business.

And fear isn't your only adversary here. Friendship or familiarity—what we call "comfort buying"—can be just as detrimental to your security well-being.

Much in the way your favorite comfort food tastes good, is convenient, and makes you feel better in the moment—but doesn't make you healthy—a solution you or your staff have used in the past might make you feel good because it's a known entity, but it won't make your business more secure.

LESSON #2
Product companies don't care about you.

You might spend more money and you might buy more security tools, but you have no way of knowing if you're spending in the right places or on the right things. And you have no tangible way of showing value from your investments.

As we'll find throughout this book, one of the biggest reasons the cybersecurity industry continues to fail you is because its methodologies are rooted in outdated approaches insufficient to tackle the challenges of today's evolving cyber attacks.

So why doesn't the industry change?

LESSON #3
Because this is the way it's always been done!

We know it's a terrible answer, but **the truth is the security industry profits from its own failure.**

It's the foundation of a vicious cycle directly resulting from the failure to prevent attacks from executing in the first place—which is, after all, the *primary job* of cybersecurity. When breaches occur, we buy more stuff, more of the tools that are already failing us.

Lots companies besides Sophos enjoyed huge financial gains in the wake of WannaCry's destruction

[3] Fletcher, Nick and Haroon Siddique. "Cybersecurity stocks boom after ransomware attack." The Guardian. May 16, 2017.

too: Cyber consultancy ECSC surged 42 percent; FireEye's prices raised seven percent; NCC group added five percent to its valuation; Symantec was up by more than three percent; and Palo Alto Networks gained 2.7 percent.[3]

LESSON #4

Security companies get richer, but you don't get any safer.

As long as companies continue to make money off of the old way of doing business—that is, profiting infinitely more from the work related to incident response than in building solutions that prevent attacks from executing—it'll always be in the industry's best interest to sell and profit based on FUD, familiarity, and failure.

We know hackers are always evolving and becoming more sophisticated, so it's time the security industry focus efforts on more sophisticated methods of prevention and protection.

Meanwhile, you don't have to accept the lies.

WHAT YOU CAN DO TODAY

- ☑ **Define what business value means to your organization and ensure security purchases are aligned to your business outcomes**
- ☑ **Don't let vendor hype steer your cyber strategy**
- ☑ **Don't select solutions based on fear or familiarity**
- ☑ **Always ask vendors how their solution solves your specific business need**
- ☑ **Always bring rationality and accountability into your decision-making process**

You can break the twin cycles of buying from fear or comfort by removing emotion from the selection process, vetting solutions to ensure they meet your business as well as your security goals, and understanding the totality of your business risk. You can evolve from the outside-in buy strategies favored by the industry to an inside-out methodology that serves your business needs first by cutting through product pitches and marketing claims, and then by building or revamping your security program with your business drivers at the core.

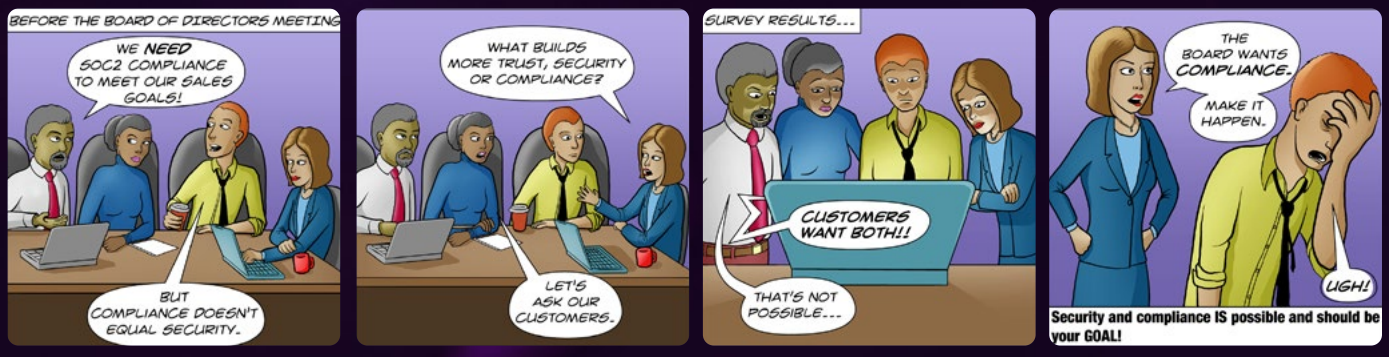
LESSON #5

There are no silver bullets in security. Define the business outcomes a successful solution must provide before you buy.

CHAPTER

2

THE BATTLE OF *SECURITY* VS. *COMPLIANCE*



UNF**KING CYBERSECURITY by CYVATAR.AI

Protecting data privacy is real, and protecting personally identifiable information (PII) is often a matter of complying with legal and regulatory requirements as much as it is a security concern. For many organizations, navigating between the two can seem like being forced to choose between Scylla and Charybdis, but we'll show you in this chapter how you can have both without sacrificing the requirements of either one.

Maybe your industry or business is young and you don't yet see where cybersecurity fits in the ecosystem; maybe you're too small an organization to have set aside budget dollars for cyber solutions; maybe you're in a compliance-driven organization that prioritizes compliance requirements over security investments.

These are situations we see every day. It's not at all uncommon for executives to find themselves without the time to understand security or for organizations to lack the staff required to focus on it. Security functionality often gets bumped, especially in development, in favor of the features and capabilities customers ask for, particularly in high-growth sectors like technology and in compliance-driven industries like financial services and healthcare.

And they're not alone.

61% of corporate board members admit they would compromise on cybersecurity in order to achieve a business objective.[4]

The downside is, of course, that only 16 percent of executive leaders say their companies are well prepared to deal with cyber risk. A recent McKinsey report notes that growth in most industries depends on new technology, such as artificial intelligence, advanced analytics, and the Internet of Things (IoT), which may expose companies to new types of cyber risk from new or evolving threat vectors.[5]

To bridge the gap, you may decide to beef up on compliance. However, **companies invest in compliance activities to follow various laws and regulations—not necessarily to improve their security posture.**

Regulations such as SOC2, GDPR, CCPA, PCI, HIPAA, Sarbanes-Oxley, and more force organizations to meet multiple—even competing—compliance challenges that each require constant monitoring, frequent audits, and professional staff and technologies, which drives up the cost to stay in compliance.[6] As a result, many companies tend to decouple compliance requirements from their security strategy, **putting these two critical safeguards in competition with each other and nearly always sacrificing a strong security posture in favor of fulfilling compliance needs.** Compliance becomes the entire security strategy.

Putting compliance ahead of security probably makes some intuitive sense for many executives—after all, laws including California's CCPA, New York's SHIELD Act, and Ohio's Data Protection Act are just three of the more than 150 consumer data privacy bills introduced in U.S. state legislatures last year—and there's a federal consumer data privacy act in the works too.

Additionally, the consequences of non-compliance can be costly. Business disruption represents the most expensive consequence of compliance failure, followed by fines, penalties, and other settlement costs:[7]

- Infringements under GDPR carry a maximum fine of €20 million (about $27 million) or 4% of annual revenue, whichever is greater.
- Fines related to intentional CCPA violations can cost as much as $7,500 per affected customer; the fine for negligent incidents can cost up to $2,500 each.

[4] National Association of Corporate Directors. "Business Model Disruptions, Slowing Global Economy Top List of Corporate Directors' Concerns For 2020." Globe Newswire. December 11, 2019.
[5] McKinsey & Company. "Perspectives on Transforming Cybersecurity." March 2019.
[6] Ponemon Institute. "The True Cost of Compliance with Data Protection Regulations." December 2016.

— Meeting or maintaining compliance by industry sector costs organizations between $7.7 million (in sectors like media) and $30.9 million (in financial services).

— Smaller organizations have higher per capita costs of compliance: Costs are highest for organizations with fewer than 1,000 employees and lowest for organizations with 75,000 or more employees.

As compelling as the data seems, **compliance divorced from security is just a stop-gap measure, even if it fosters trust with customers.** Trust is one of the biggest reasons compliance-centric programs are popular. Trust brings confidence. Trust brings revenue.

But when companies get into the habit of continually compiling new cybersecurity checklists, they create an **undue focus on formal compliance rather than on cyber resilience.** Even when all boxes on the checklist are ticked, the company may be no less vulnerable to attacks than before.[8]

In the meantime, security itself becomes an afterthought, an add-on to business goals, rather than a critical, integral part of them, making it impossible for security to act as a catalyst for sales and revenue growth.

The add-on approach may even become a drag on business velocity by increasing user friction or delaying time to market for new product features. When secure systems are not usable, there is a risk that users may try to avoid them or disable the security features entirely. As one CISO put it, "If you build an overly burdensome solution, users will do their best to circumvent it."

People may also use security features incorrectly or make errors that compromise security, despite that nearly 75 percent of respondents to a recent *Dark Reading* poll say their organizations would be safer if security measures were easier for end users.[9]

By separating compliance from a security strategy, we create a "check-box" mentality and foster an environment of more or less following the letter of various requirements while missing their spirit entirely: Thousands of companies become compliant but still get breached.

LESSON #6

Done right, compliance simply becomes the byproduct of a sound security strategy.

Recent research shows that the higher an organization's Security Effectiveness Score (or SES, a measure of its ability to meet reasonable security objectives), the more effective the organization is in protecting sensitive information, assets, and critical infrastructure. **The higher your SES score, the lower your compliance costs.**[10]

[7] Data adapted from Ponemon Institute. "The True Cost of Compliance with Data Protection Regulations." December 2016, and Crane, Casey. "15 Auto Dealership Cybersecurity Statistics That Will Drive You To Action." Cyber Crime Magazine. February 14, 2020, .
[8] Op cit. Ponemon Institute.
[9] Chickowski, Ericka. "User-Friendly Cybersecurity: Is a Better UX the Key to a Better Defense?" Dark Reading. April 30, 2020,.
[10] Op cit. Ponemon Institute.

WHAT YOU CAN DO TODAY

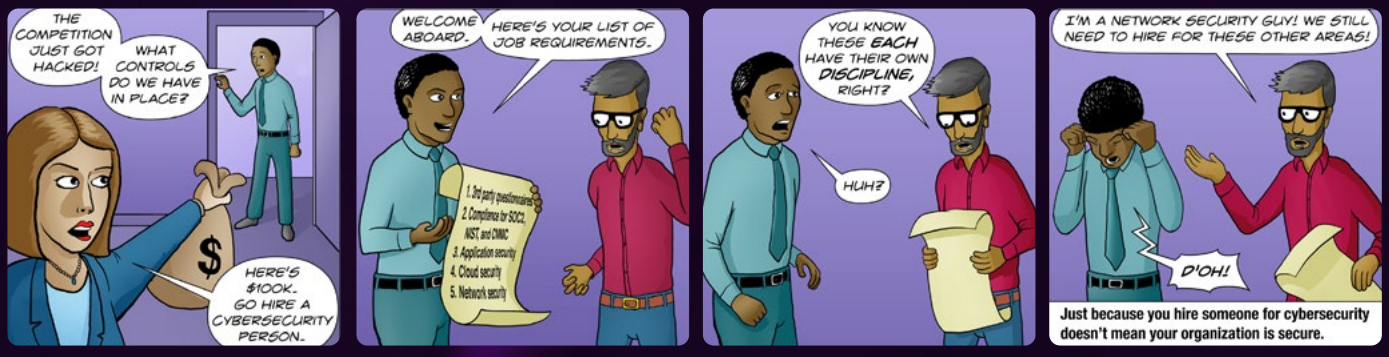
- **Always approach security as an integrated exercise that spans all of your business goals—including compliance**
- **Never force yourself to choose between security and compliance—you can easily have both**

Remember, a successful, integrated security strategy will deliver the compliance requirements you need and support a public-facing security stance that builds inherent trust with customers, leading to long-term revenue growth and increased security confidence.

CHAPTER

3

MISALIGNED *RESOURCES*



Cybersecurity as a discipline has continued to grow over the past few decades and the IT professionals who have chosen to specialize in it have become some of the most sought after workers in technology. Like any scarce resource—think of the current housing boom of rapidly rising prices and historically low inventory—**demand for skilled cyber practitioners far outpaces the number of qualified professionals to meet it, driving up the cost to hire and retain those resources in-house and making it virtually impossible for small and medium-size businesses to compete for them.** Even on the consultancy side, larger organizations with deeper pockets snap up all the talent they can regardless of cost.

And while it may be true that there's an abundance of cybersecurity training and related courses available, there's no substitute for hands-on experience. Proven expertise is still the only real measure of capability, shrinking the talent pool further to only those practitioners who've done cyber battle out here, in the real world, for real companies.

The good news for companies too young or too small to compete for these rare resources is that no matter how good a cybersecurity professional is, there will always be a need to understand the discrete business environment unique to every organization.

And that helps level the playing field for the rest of us.

The more technically trained cyber practitioners are, the narrower their skillsets typically become and the more focused they stay on solving problems with a technical win rather than a business one, making it harder for them to invest in the business acumen needed to, for example, drive more sales by making the business secure.

The same is also generally true of your business professionals. Business-minded talent that doesn't have an understanding of the technologies required to propel your organization forward can breed a culture of analysis paralysis, extended proof-of-concept (POC) engagements, and longer time to value. They also struggle to win the trust of your technology experts because they don't understand cyber, making company-wide security challenging and out of sync with your business goals.

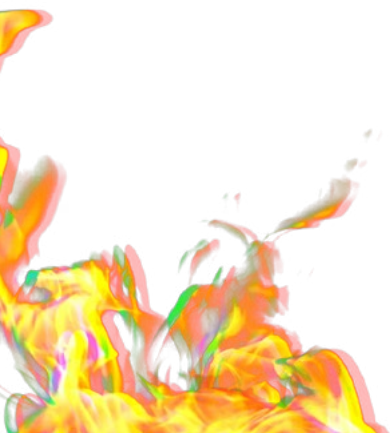
THE TIME IT TAKES TO FULLY UNDERSTAND BOTH THE TECHNICAL AND BUSINESS ASPECTS OF A GIVEN COMPANY MAKES IT DIFFICULT FOR EVEN THE MOST TALENTED OF PRACTITIONERS TO HAVE A QUICK IMPACT ON THE IMPROVEMENT OF THE SECURITY ENVIRONMENT.

LESSON #7

Discord between business and technology personnel, particularly when they lack the political acumen necessary to understand each other's motivations, makes it easy for security practitioners to wield a big stick, essentially threatening their colleagues on the other side of the table with a do-what-we-want-or-else approach that perpetuates buying new solutions out of fear of being breached.

It also alienates security teams from other parts of the organization, damaging important interdepartmental relationships that become very difficult to repair.

By fostering genuine partnerships between your business and technology experts, you'll benefit from a stronger, more resilient program intertwined with your overall business goals, giving you a leg up on companies with top security talent likely to be divorced from the day-to-day business drivers of their organizations.



WHAT YOU CAN DO TODAY

- **Introduce and support a culture that rewards collaboration throughout the organization**
- **Strike a balance between your business and security goals rather than permit them to compete with each other**
- **Promote talent from other parts of the organization—perhaps with risk, fraud, or audit experience—that understands your business drivers and success metrics and grasps the challenges inherent in your industry, and teach them the language of cybersecurity**
- **Up- or cross-train junior hires and groom them for careers in cybersecurity: Younger hires are likely more eager to build their business knowledge and security acumen in tandem, again allowing you to build a security program with more embedded resilience and relevance than traditional approaches**
- **Engage external resources to help you build and manage an outsourced security function without compromising a strong security posture or necessary business outcomes**

You may consider investing in a position like a virtual chief information security officer (vCISO) to manage basic security elements:

- **Inventory, patching, and access control**
- **Risk management**
- **Broad-based security expertise**
- **The ability to make effective risk and value decisions**
- **Strong communication and influencing abilities**
- **Good interpersonal skills and specialized security knowledge: A healthcare unit needs a security expert that understands HIPAA, while a retail banking unit requires security talent with a keen understanding of PCI.**[11]

Hiring a one-time consultant or team of consultants to assess your needs and provide a list of recommendations won't do the trick, however. Whether you require a security mentor to make immediate improvements to your security stack; professionals from several practice areas to train less experienced members of your team; or help selecting, implementaining, or maintaining security tools, consider thoughtfully what approaches are most in line with your business goals to allow you to cover the greatest number of requirements for the least amount of operating expenditures.

LESSON #8

Outcomes of successful security should not fall under the purview of the security team alone.

Cross-functional and cross-departmental cooperation across Security, IT, Development, Risk, Sales, and Finance are necessary if cyber protections are to be completed successfully.

[11] These are the same basic skills recommended for hiring what Equifax calls a "business information security officer," but without the negative connotations sometimes associated with that role. Fazzini, Kate. "New Equifax CISO Tightens Structure Post-Breach." WSJ Pro Cybersecurity. September 6, 2018.

CHAPTER

4

PRODUCT AND SERVICES COMPANIES REALLY *DON'T* CARE ABOUT YOU

UNF**KING CYBERSECURITY by CYVATAR.AI

But it begs the question: What do they care about? There's no single answer.

Some companies care about changing the world with groundbreaking technologies. Some focus on amassing as much profit as possible as quickly as they can. Still others simply want to meet their company's goals, be they large or small, quarter after quarter. There are as many answers to the question as there are companies building security solutions.

But one thing's for certain: Providers never begin with your business needs in mind, and cybersecurity is never about just one product or service anyway.

LESSON #9

Successful security programs are built on the three pillars of people, process, and technology.

If you look no further than technology, you may find you've invested in only one-third of a complete solution; without the right people and proven security process, the best technology on the market still leaves you vulnerable to attack.

Cybersecurity author and researcher Greg Scott sums up the dilemma well: "Big companies and small companies and everyone else are already in the crossfire of a cyber war. It's not burgeoning, it's already here. And it's not just between the U.S. and China, it's between everyone who has data, and lots of attackers who want to steal it. Why would anyone be surprised that the enemies of the United States try to steal secrets from U.S. companies?" [12]

Whether it's basic IT hygiene (such as patching vulnerabilities or comprehensive asset management) or user education (including better email protections or password habits), we know from the post mortem of every successful breach that the devil is in the details and it's from the details that our security devils must be exorcised and exterminated.

The question we should all ask, says Scott, is why our companies are still so unprepared, even after years of headlines? Because most security providers aren't willing or don't have the resources to provide all three foundational pillars of cybersecurity. Breaches from Yahoo to SolarWinds all resulted, on one level or another, from a fundamental gap in the security environment resulting from inadequate technology, talent, or controls.

SPOTLIGHT ON MARRIOTT:

A Double Dose of Failure

Analysts estimate the sizable Marriott breach of 2018 was the second biggest ever, behind only Yahoo and ahead of third-place Equifax. Nearly 400 million Marriott customers were affected, their personal information compromised. Notable points include:[13]

- It took Marriott 4 years to detect the breach
- Hackers operated undetected in hotel systems for more than 2 years
- The company's due diligence during the Starwood acquisition did not uncover the incursion
- Marriott did not publicly disclose the breach for two months after it was discovered

The breach exposed up to:

- 383 million guest records
- 18.5 million encrypted passport numbers
- 5.25 million unencrypted passport numbers
- 9.1 million encrypted payment card numbers
- 385,000 card numbers

[12] Nohe, Patrick. "Autopsying the Marriott Data Breach: This is why insurance matters." Hashed Out. March 22, 2019.
[13] Data from both lists adapted from Cimpanu, Catalin. "Marriott CEO shares post-mortem on last year's hack." ZDNet. March 8, 2019, and Op cit. "Autopsying Marriott."

The breach was discovered when an administrator's account was used to make an unusual database query—but the query was not made by the individual whose credentials were used. The causes of the breach were at least twofold: a remote access trojan (or RAT), malware that allows an attacker to covertly access, surveil, or gain control over a computer; and Mimikatz, a penetration-testing tool that searches a device's memory for usernames and passwords. Mimikatz was most likely used to help hackers acquire passwords for other Starwood systems and help them move throughout the entire IT network.[14]

Now here's the heartbreak: All of these attack vectors are as old as cybersecurity itself. This was not a sophisticated modern-day attack; it was old school, with decades-old technology and brute force execution. Even without the right people or controls in place, Starwood Marriott ought to have been better protected—it wouldn't have been that hard.

Nevertheless, uncovering the full scope of the attack took significant forensic work, and disclosing the breach was also a massive effort. The latter involved notifying the FBI, all 50 U.S. state attorneys general, the FTC, the SEC, regulators in 20 different countries, four major payment card networks and their credit card processing vendors, and three U.S. credit reporting agencies.

An investigative team working on behalf of payment card networks is still looking into the hack independently of Marriott's team and U.S. authorities.[15] As one commentator put it, "Marriott's security posture was likely poor, but its response was worse."

Worse still, **the beleaguered hotel giant did not become more secure post-breach: Within 16 short months it was hacked again, exposing the personal information of more than 5.2 million users of Bonvoy, the Marriott loyalty app.**

This time, the attack infiltrated a third-party system used to provide guest services. Bad actors stole the login credentials of two employees with access to the system which they then used to expose customer contact details including names, mailing addresses, email addresses, phone numbers, birthdays, gender, and company names.

SPOTLIGHT ON EQUIFAX:

We Failed to Protect the Data of 148 Million Americans, but Hey Presto! Our Profit Margin Rose by 127%!

Human error and a reckless approach to security over many years were at the root of this notorious hack according to former CEO Richard Smith, who left the company in the aftermath of the breach. Smith met with Equifax security and IT teams just four times a year to understand the defenses necessary to protect the PII of more than half the country's citizens.

Poor data hygiene, permissive access controls, and an open network architecture gave hackers all the help they needed to pilfer the crown jewels of U.S. consumer data.[16]

The list of failures is staggering: flawed, inadequate patching protocols. Lack of robust and consistent data encryption. Impotent vulnerability scanning tools. Security personnel who dropped the ball.

[14] Op cit. "Marriott CEO."
[15] Ibid.

Any one of these snafus might have been enough to invite an attack, but that this entirely preventable breach was caused by the failure of one person to implement a critical patch (which the U.S. Computer Emergency Response Team provided to address an open-source software vulnerability)[17] and that for months the company's security systems failed to flag it are so egregious there's nothing to be said in its defense.

Massive fines and other forms of restitution have been levied against Equifax as a result of the breach: upwards of $2 billion based on some estimates, including $1.25 billion already spent on new security and technology investments but exclusive of the additional $1 billion the company must spend over the next five years to improve its data security.[18]

Nevertheless, Equifax's profit margin is healthy—up 127% as of December 2020—even though its approach to breach remediation does little to inspire confidence that it will be any better protected next time around.

Here's why. Six of the 11 remedial recommendations given to Equifax by a leading cybersecurity consultancy included the purchase of the new security and technology investments mentioned above *despite the failure of many similar tools to prevent, detect, or contain the breach in the first place.*

The consultants did include a few process recommendations as well,[19] but nothing in their list of remedies included critical people-focused fixes. They focused instead on the one area we know is a weak link and ignored a full third of the components required for successful cybersecurity.

Other security pundits agree. Reporter Patrick Nohe, writing for *Hashed Out*, spoke to one chief executive who said:

> *The state of corporate cyber-defense in the U.S. is at best, inconsistent, and at worst broadly mediocre.* ***That is not to say some companies don't spend a lot of money on security. But often they spend it on buying the latest shiny new cyber tool, rather than focusing on developing a broad risk-based approach…****Security budgets are delegated to the CISO, who often sits within the IT function, meaning solutions tend to be tech- rather than people-focused…****No technology can, on its own, ring-fence our data."*[20]

[16] Adapted from Newman, Lily Hay. "Equifax's Security Overhaul, a Year After Its Epic Breach." *Wired*. July 25, 2018.
[17] Op cit. "New Equifax CEO."
[18] Brumfield, Cynthia. "Equifax's data breach disaster: Will it change executive attitudes toward security?" CSO. July 24, 2019.
[19] U.S. House of Representatives Committee on Oversight and Government Reform. "The Equifax Data Breach." Majority Staff Report, 115th Congress. December 2018, Page 85.
[20] Op cit. "Autopsying Marriott."

ASK YOUR *VENDOR:*

Rather than try to guess a security provider's motives, here are 10 questions you can ask to ensure your organization is—and remains—protected:

1. Do you provide services as well as technology?
2. What recourse do we have if your technology fails and we are breached?
3. Do you offer incident response services?
4. Do you provide continuous vulnerability scanning?
5. Do you provide regular patching services?
6. Do you provide ongoing remediation?
7. Do you provide active noise filtration and alert management to reduce false positives and support effective issues resolution?
8. Do you make more money/profit from selling services post-breach or from preventive technologies?
9. Can you provide or train additional human resources to keep my data safe?
10. Can you provide customer contact information so I can check references?

Taking the time to ask these questions can help you avoid the fate of the 92% of respondents to a recent Debate Security survey who identified a deleterious and deep-seated "information asymmetry" between buyers and sellers of security solutions.[21]

After all, security is a process, not a product.[22] We learned long ago that finance teams did not, could not, operate in a silo, that they were intricately intertwined throughout the whole organization, and the same approach should be taken with security.

For ease of internal reporting and external transparency, it makes sense to have a named owner of the security process, but you should not take ownership to mean sole responsibility. You will reap more long-term value by thinking of security as a program of work with a central coordination point and multiple areas of organizational responsibility where each is accountable for a specific piece of the program.

[21] Infographic available here.
[22] Schneier, Bruce. "The Process of Security." Schneier on Security. April 2000.

WHAT YOU CAN DO TODAY

- ☑ **Always evaluate vendors on all three pillars of cybersecurity, not just on their technology offering**
- ☑ **Always maintain an ongoing process to protect and maintain sensitive data**
- ☑ **Never treat security or compliance as intermittent events; support for them must be continuous**
- ☑ **Keep all software and systems up to date**
- ☑ **Continuously scan your business systems for vulnerabilities**
- ☑ **Patch all vulnerabilities upon discovery**
- ☑ **Ask current customers what value they see from their providers, what challenges they've faced, and whether they'd do it differently if they had to do it again**

LESSON #10

Product companies wouldn't keep making money they didn't earn if buyers held them accountable.

Always remember: It's the product or services company's responsibility to prove its value. Ask for proof points, look carefully at their methodology to ensure compatibility with your business goals, and always take the time to talk to their customers.

Consider carefully the people, process, and technology you need to extract product value—a company can sell you anything, but without all three security pillars in place, you could become the next Equifax.

CHAPTER

5

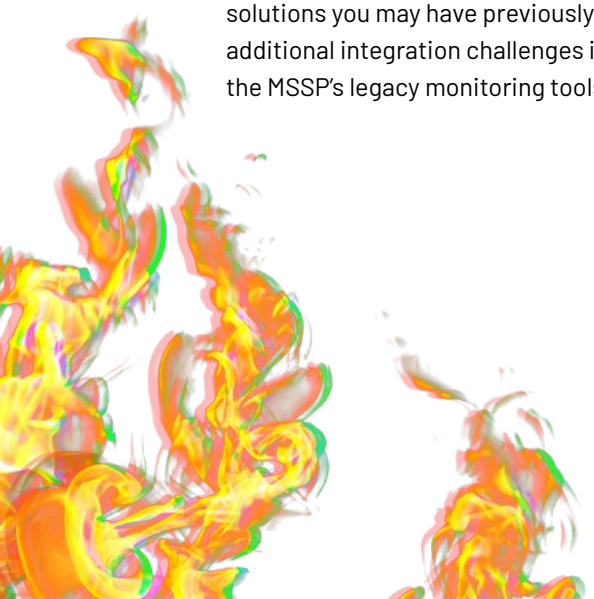
MANAGED SERVICES PROVIDERS LEAVE YOU *HOLDING THE BAG*

UNF**KING CYBERSECURITY by CYVATAR.AI

When faced with obstacles to achieving successful security outcomes like those we've discussed so far, you may decide to turn to the promise of market aggregators, to managed security services providers (MSSPs) or value-added resellers (VARs), to help you sift through the deluge of products available, implement solutions, or assess existing cyber investments. These engagements can be costly relative to results, and all too often you're the one who'll be left holding the bag when the partnership fails to produce the promised outcomes.

The failure of MSSPs to live up to their promise lies chiefly in two areas: their inability to integrate into the entirety of their customers' security and IT environments and the lack of clearly defined responsibilities related to the maintenance and management of the discrete tools running in those environments.

MSSPs typically select specific security solutions familiar to or preferred by themselves, rather than choosing solutions best suited to your company's unique requirements, making it difficult to integrate fully—let alone easily or seamlessly—into your IT ecosystem. Any SaaS-based or non-traditional solutions you may have previously purchased pose additional integration challenges in order to work with the MSSP's legacy monitoring tools.

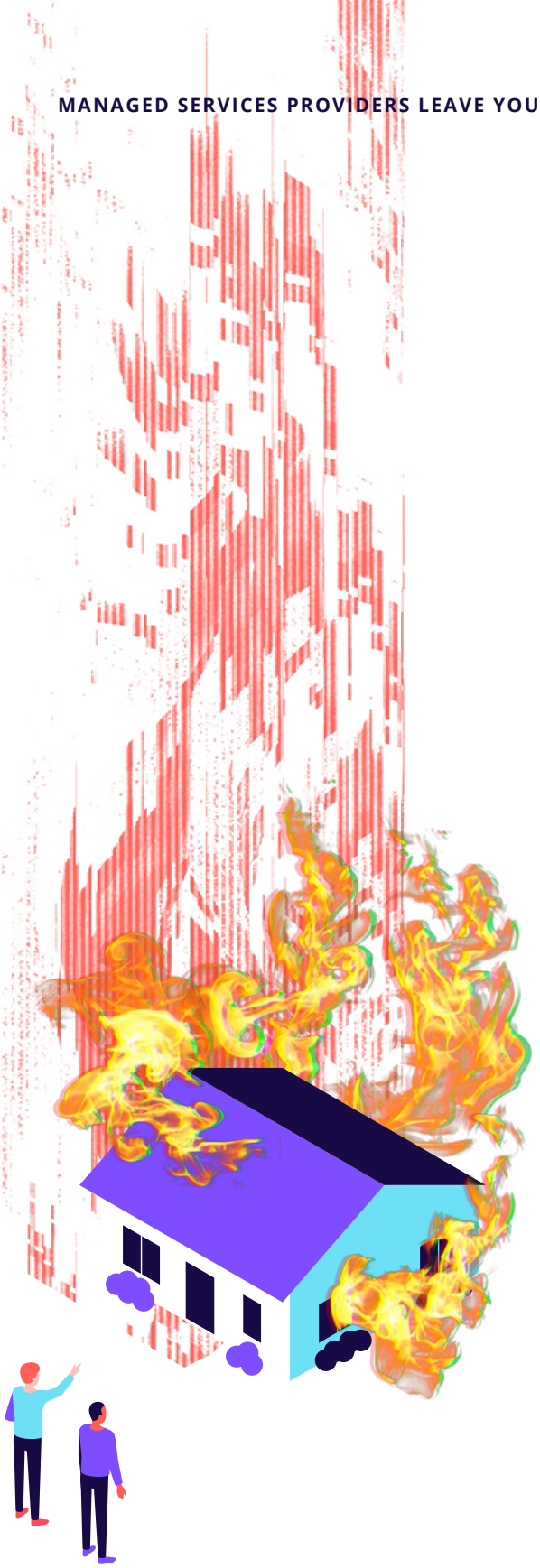


The disparity among these various investments ought to be resolved up front in the MSSP agreement, but that's rarely the case. You're more likely to believe the MSSP is responsible for managing the security and technology solutions you own in addition to anything new they introduce, but if the MSSP is incapable of integrating with your existing tools, visibility and coverage gaps will leave you more vulnerable to cyber threats than you were before the engagement.

Without continuous visibility and remediation across the entire security environment, issues and alerts generated by the MSSP are likely to yield a high number of false-positives, the investigation and remediation of which then falls to you to resolve:[23]

- **99% of cybersecurity professionals say high alert volumes cause problems for staff**
- **70% say the volume of alerts has more than doubled since 2015**
- **85% struggle to cope with the near-constant barrage of such alerts**
- **83% say their teams experience alert fatigue**

[23] Data adapted from Scroxton, Alex. "Majority of security pros fed up with alert fatigue." Computer Weekly. July 9, 2020.



Your MSSP provides just such a barrage of security alerts, which is the equivalent of telling you your house is on fire. They shout! They point! They incite panic! You look wildly to them for help, but their buckets hold no water. They offer to help clean up the mess—after your house has burned down—which incidentally costs you more than what you paid them to tell you the house was burning. Importantly, nothing in their services agreement holds them accountable for preventing your house from catching fire in the first place.

It's possible your MSSP will recommend some type of automated solution that provides real-time analysis of security, but "analysis" is just a fancy word for alerts with context; it will not prevent or remediate an attack. Your house will still be a pile of ash, and you will still have to pay someone to clean it up and rebuild it.

LESSON #11

Most MSSPs only provide security monitoring services, which puts the burden of investigation, prioritization, and remediation on you—a burden no organization without a sound understanding of security, a solid process roadmap, and technically skilled resources is truly equipped to handle.

Never forget that, pre- or post-breach, all of the solutions in your security environment need to be managed and maintained continuously. It's not often clear what the MSSP is responsible for and what you

and your team must manage, and if no one is clearly responsible for monitoring and reporting on every solution, there's a good chance there are gaps where no one is minding critical parts of the store, even though you may assume the MSSP is responsible for covering them, particularly when a breach occurs.

VARs, also known as channel partners, pose different risks. They are mostly transaction-based and have their own agendas; they work for outside organizations and are not your employees. Therefore, they make choices that are in their best interests or otherwise benefit the companies that employ them rather than recommending the solutions best suited to your technology and business needs.

VARs are coin-operated, incented by product company SPIFFs and whatever activities are beneficial or profitable to them. That is, whatever makes them the most money.

To achieve the outcomes you expect and need with MSSPs or VARs will require heavy lifting from you and your organization, either heading into the engagement, throughout it, or both.

MSSPs will need to be integrated with and have visibility into all of your internal processes and existing technology solutions to eliminate the reporting of false positives, deliver meaningful alerts, and provide threat remediation.

VARs, unfortunately, offer even less value. Their transactional nature means they will always only offer you the solutions that best suit them and their needs rather than yours.

WHAT YOU CAN DO TODAY

- **Don't be afraid to hold your MSSPs and VARs to account**
- **Ask them if they profit more from preventive security measures or incident response services**
- **Challenge them to remediate any alerts they generate**
- **Challenge them to prevent attacks, not just respond to them**
- **Challenge them to make sure they're obligated to help if what they sell you fails**
- **Challenge them to measure the success of your security environment in a remediated or "clean" state, not by the number of alerts they send you**

CHAPTER

6

SECURITY PRODUCTS BECOME *SHELFWARE*

UNF**KING CYBERSECURITY by CYVATAR.AI

Shelfware is a term used to describe anything that gets figuratively left on a shelf or is rarely used in day-to-day activities—the unfortunate fate of many security technologies. The promise of a silver bullet or some miraculous degree of protection often rapidly diminishes (if it doesn't disappear outright) once the product has been purchased, leaving you with a fraction of the capability you paid for.

Security tools become shelfware for a number of reasons:

1. Because buyers panic after a breach and make decisions based on fear
2. Because the industry encourages purchases in pursuit of the hottest new thing while the tools you already have languish
3. Because the majority of budget allocation by product companies is targeted toward new customer acquisition rather than ensuring their products are installed and configured correctly

Fear and panic we've covered, so let's take a look at the other fails.

The product company mentality of pushing through a sale based on marketing hype is not much different from an impulse purchase made from a late-night infomercial or TV shopping channel. Remember the Flowbee? No messy trimmings! The Veg-O-Matic? It slices! It dices! It makes julienne fries! Both came with a flurry of extra gadgets you neither wanted nor needed—but only if you bought within 10 minutes of the broadcast.

Sounds an awful lot like security hype, doesn't it? Here are just a few of our favorites, from real providers, but the emphasis and commentary are ours:

"Market-leading NGAV *and* integrated threat intelligence *and* immediate response."
It slices! It dices! But wait—what's a NGAV?!

"First cloud-native endpoint protection platform."
And that makes my business more secure how?!

"Cloud-native, SaaS security platform and intelligence-driven security."
Well I'm pretty sure I don't want stupidity-driven security?!

"The only comprehensive cloud-native security platform."
Aren't there two others in this short list alone?!

"Rapidly onboard remote users at scale with [cloud] access & next-generation firewall."
And that protects my data how?!

"Autonomous AI endpoint protection."
Okay, so it's smart and plays by its own rules. Is that even a good idea?!

"Speed your digital reinvention by infusing the intelligence of AI and the agility of hybrid cloud to modernize, predict, automate and secure your business."
Is digital transformation over already? And isn't AI intelligent by definition?!

"Detect and protect against known and unknown vulnerabilities with cross-generational protection techniques."
How can cross-generational techniques possibly improve my security?!

"The only security company laser-focused on striking down targeted cyber threats."
Now hang on—isn't that EVERY security company? I mean, isn't that what the 4000+ tools are for?!

We could do this all day.

All of these providers are saying the same thing: You will be hacked. So what, exactly, are you paying for?

If you don't look too closely or think too hard, some of this provider gobbledegook starts to sound pretty good, and the next thing you know you're hooked. Fast-forward six or 12 months and there the product lies, like your Flowbee, on the shelf or in the drawer adding zero value. You've likely bought other solutions since then too, of varying degrees of usefulness, sitting side by side with all of your "old" tools.

Of course, your average cyber purchases cost a great deal more than infomercial products, and worse, they give you a false sense of security based on stated value they do not actually provide.

Sadly, the rabid focus of product companies to sign up as many new customers as quickly and as often as they can has a similar result: lots of money for them, insufficient cyber protection for you.

LESSON #12

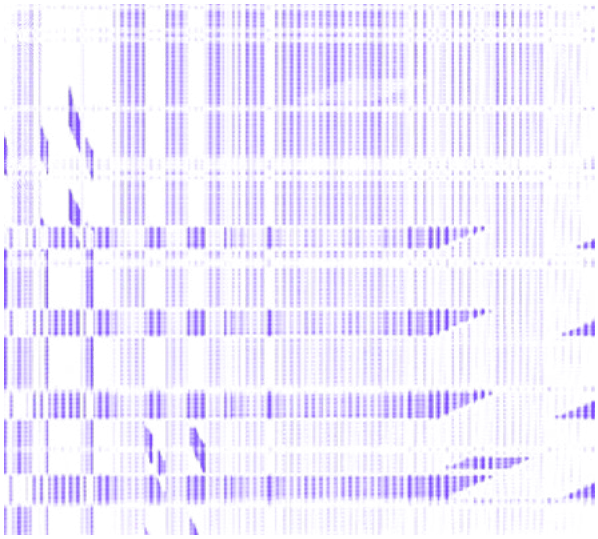
New customer acquisition is a vital part of the elaborate lie the security industry propagates to entice you to embrace the hype and drink the proverbial Kool-Aid. But it's up to you to figure out how to make the technology work.

Said another way, product companies excel at the sale; however, once you've signed on the dotted line, you enter what's known as the "dead period" and the vendor feels no need to continue to demonstrate value—they've already moved on to the next buyer.

How many times have you bought a product and not heard back from the seller until your contract was up for renewal? How often did you actually renew? Chances are, you either:

1. **Renewed because it was easier than replacing the tool, hoping you'd see value somewhere down the line; or**
2. **Didn't renew and started the whole process over again with a new vendor.**

Either way, you were sucked into the vicious cycle of buying more products that fail to keep you safe.



THREE-YEAR TECHNOLOGY LIFECYCLE

1. **You buy a cool technology**
2. **It creates more alerts and gives you visibility**
3. **It does not remediate what it finds**
4. **Your staff did not implement it properly**
5. **One year later, you find minimal value/outcome/results**
6. **The next year you rip and replace it for the next cool tech**
7. **In year three you roll out the next new cool tech and start the cycle again**

Again, selecting a cybersecurity solution is more than simply buying a product, especially if you never hear from the vendor again until it's time to renew. You need to ensure your tools are installed and configured correctly and that your issues are being remediated as they are found. **You need the confidence that your security requirements are being met around the clock.**

Your needs change as your business grows, and your security solutions should be flexible enough to change with them so that you can continuously remediate new risks and ensure you always receive measurable outcomes from your solutions—that's where ICARM comes in.

ICARM, or installation, configuration, assessment, remediation, and maintenance, is a methodology for achieving smarter, clearly quantifiable solutions. And in the crowded and noisy security space, the need for you to show value from your technology spend is a top priority.

LESSON #13

Without ICARM, you run the risk of accumulating shelfware.

We spoke at the beginning of the book about the security industry's predilection for peddling FUD as a smokescreen tactic, playing off a perceived need that has been created by external influences. The current hype around advanced persistent threats, cross-site scripting, or ransomware attacks, for example, may succeed in keeping you up at night, making the promise of any tool purporting to protect effectively against these threats enticing indeed. Don't be fooled.

Because few companies disclose the complexity, difficulty, or sheer effort required to implement and maintain their solutions effectively.

And that makes sense on one level—when was the last time you ran out to buy something you knew would make your life more difficult? But it's also dishonest, and dangerous, because people's lives and livelihoods may be at stake when security solutions fail to live up to their promise.

The fact that so many security offerings require a 24/7 SOC or other hefty investments to become fully operational is not information readily offered during the sales cycle. And of course, once the solution is brought in-house and its failings made manifest, it's

Much in the way making a purchase out of fear opens the door to new risk, improperly or partially installed solutions also introduce risk to the security environment by creating functionality and integration gaps that are easy for threat actors to exploit.

frequently left to sit on the shelf, without the care and feeding (ICARM) it needs, until it slowly becomes obsolete, never having delivered much (if any) value.

If we continue to choose security solutions to solve for perceived risk—rather than actual risk—and if we fail to define clearly the outcomes we require, what incentive will product companies have to do better, to make good on their many, many promises?

Without ICARM, a clear security strategy, and a process roadmap in place, we remain trapped in an expensive cycle of buying what we think we need or have been told we need and every shiny new tool that makes its way to market offers more of the same fresh, false temptation that has failed us every time.

WHAT YOU CAN DO TODAY

Before you buy, take the time to determine the resources required to install, configure, assess, remediate, and maintain the solution you're evaluating so that you can achieve smarter, measurable outcomes that enable you to get to security compliance and cyber-attack protection faster and more efficiently—and show value from your security stack.

Odds are, though, you're going to need some help:

- **Can you accurately estimate what it will cost to do the work yourself?**
- **Do you have the in-house expertise to implement ICARM methodology?**
- **Have you completed successful implementations before, or do you have shelfware? (And be honest, because we all have shelfware somewhere!)**

Think of the household projects you've attempted yourself and how frequently you received a better end result by calling a professional—well the same is true for cybersecurity. What looks like cost savings at the outset could wind up becoming a whole lot more expensive down the road.

There are almost always unforeseen costs associated with tackling security implementations on your own, up to and including the loss of your job or your company's reputation in the aftermath of a breach.

Ask the Vendor Round 2: Here are 6 questions to ask your security provider to determine if they can support the ICARM approach:

1. Can you install and configure the product for me and ensure it works as promised?
2. Can you train my staff to manage and maintain it, or do you manage and maintain it for us?
3. Can you assess my environment to identify risks and vulnerabilities?
4. Can you remediate the risks you identify rather than just report them?
5. Can you provide continuous monitoring, assessments, and monthly executive-level reporting?
6. How much do your services cost? Are they included with the price of the software?

CHAPTER

7

PEN TESTS AND LONG POCs STILL GET YOU *BREACHED*

UNF**KING CYBERSECURITY by CYVATAR.AI

LIKE A POLL USED TO MEASURE POLITICAL SENTIMENT, TRADITIONAL PENETRATION TESTS ONLY REFLECT THE STATE OF A SECURITY ENVIRONMENT AT A SPECIFIC POINT IN TIME.

They are not designed to anticipate future behaviors or predict likely outcomes. In fact, given the rapid pace of change in most organizations and the dynamic fluidity of evolving threat vectors, at best, a pen test will give you little more than any other assessment tool, leaving you with identified vulnerabilities you then have to figure out how to remediate.

Software updates and new releases happen frequently—multiple times a day for companies that are heavily DevOps-oriented and many times a year for less sophisticated organizations[24]—making it impossible for a pen test to accurately reflect threats and vulnerabilities in your environment at any time other than when the test itself is administered.

The truth is, an absence of business context has plagued pen testing activity for a long time. The lack of knowledge about a particular customer or environment leads to the reporting of factors that often do not pose a genuine risk.

Add to which, the effort associated with remediating vulnerabilities and closing gaps will almost certainly fall to you and your staff, after the pen test team has gone home.

The likelihood that you will find yourself wasting time trying to fix outdated issues with old approaches is high and could be costly, without making your business safer or more resilient.

Similarly, a proof-of-concept engagement (POC) often launches to help you understand the true results you can expect from a product you have not yet purchased.

POCs are also used to compare one product to another in terms of functionality or other benefits. It's a try-before-you-buy approach and a low-risk avenue to test the efficacy of a solution that interests you.

Or is it?

POCs are a bit like window shopping at a grocery store: You can look at all the tasty food, but if you don't buy any, you starve to death.

[24] Wang, Dr Chenxi. "Pentest as a Service Impact Report: 2020." Cobalt.io.

You may feel compelled to launch a POC as a result of marketing hype or to help you determine outcomes that are wrapped in product promises but difficult to measure. Before you do, consider these three common pitfalls:

1 **Wasting time evaluating technologies that don't map to your business goals.** There's no point testing what won't produce the outcomes you need, so don't.

Cautionary Tale: A B2B technology company set a goal to fix all critical and high-priority vulnerabilities so they could reduce business risk and achieve compliance requirements faster. The outcome? They spent three months in POCs testing various vulnerability scanners, but the company overlooked the fact that for more than 90 days their vulnerabilities remained unprotected and open to exploitation by bad actors. They would have been better served getting to remediation faster, especially since vulnerability scanners differ very little from each other.

2 **Chasing features and functionality rather than pursuing your business goals.** This is the shiny objects trap—avoid it.

Cautionary Tale: A financial services company set a goal to better protect online customer data. Instead, they put security efforts on hold while they waited for upgraded protections promised by a vendor that were never delivered—that were never even built. Like the tech company that lay vulnerable for three months while evaluating new tools, this organization put sensitive customer PII at risk as they waited for promised upgrades they never received. The company believed the vendor's false promise when they should have kept their goals in mind and secured the customer data immediately.

3 **Immobilizing your organization through analysis paralysis.** In your quest for due diligence it's easy to get bogged down by data. If you keep your business goals top of mind, it will be easier to recognize when you've lost perspective.

Cautionary Tale: An automotive company set a goal to understand and secure all of their hardware and software assets—an important early step in any security strategy, because you cannot protect what you don't know you own. The company spent 18 months evaluating IT asset management products, but they became consumed by comparing various benefits among the products and could not make a decision. After nearly two years, they still cannot properly secure the network because they have not been able to make a product decision.

LESSON #14

The longer the POC, the longer your business is vulnerable.

The many months spent on POCs won't make your business more secure and won't add any value to your bottom line. In fact, you're more likely to wind up hitting the pause button on your entire strategy as you remain trapped in a feature/function bake-off that prevents you from making a decision at all.

And while you're busy getting lost in a maze of interesting features and functions, your organization lies wide open, vulnerable to cyber attack.

WHAT YOU CAN DO TODAY

If you must enter a POC engagement, do it right. Here are best practices:

- **Secure executive buy-in first, not after the POC has started**
- **Define success criteria based on your business drivers, not on technical features**
- **Limit all POCs to 30 days; challenge your vendor to prove its value in a month, or choose another vendor**
- **Identify all gaps between the testing lab and your production environment**
- **Understand how the product will be implemented to ensure it follows the ICARM approach**
- **Have internal business and technical champions defined for the lifetime of the product**
- **Establish a process to hold the vendor accountable for delivering and maintaining your defined business outcomes for as long as you own their product**

HAVE YOU EVER FALLEN INTO THE WIN-WIN TRAP?

Too often, customers look for what is known as a "technical win;" that is, they look for (and buy) products that meet their technology requirements. But because technology requirements tend to be divorced from business requirements, it's difficult for companies that have not first identified what a "business win" looks like to achieve any real value from their technology investments.

POCs, by their very nature, are designed for the technology win: You can spend months determining whether or not a solution is technologically sound, during which time the business win is sacrificed as your company remains exposed to the very risks you are trying to mitigate.

A further downside to this approach is that it puts even the technical win at risk: The IT team, happy with the results of the POC, faces an uphill battle trying to prove that the technology benefits meet the business need. If the business owners decide they do not, both you and the product company have wasted valuable time.

The features and functions that comprise a technical win will never in themselves add value to your organization. If we've said it once we've said it a thousand times: You have to tie your technology investments to your business drivers if you want to achieve the business win. And you need the right resources and controls in place to keep it.

LESSON #15

If you engage a POC, start with the business win; if you don't see a technical win within 30 days, consider walking away.

Don't waste time tumbling down the feature/function hole unless you have no other way of evaluating the differences among multiple tools—a side-by-side POC comparison should be the very last arbiter in your decision process.

CHAPTER

8

YOU DON'T BELIEVE *VALUE IS POSSIBLE*

UNF**KING CYBERSECURITY by CYVATAR.AI

So now you know the security industry has grown fat on a diet of FUD and familiarity, leveraging sensational media coverage to sell tools that claim to fix all manner of issues, many of which tend to be far removed from the overall goals of your business and almost all of which fail miserably to demonstrate meaningful value once they're purchased.

You also know you can spend vast sums of money on new technologies that often are incorrectly or only partially implemented and then a breach occurs. Suddenly the other business owners or CEO or board members want to know how an incident could possibly have happened after you invested so much in solutions that were supposed to prevent it. There are mea culpas all around, and—too often—someone's job is on the line. Ask anyone in your peer group who's been hacked.

LESSON #16

Failing to get value from cybersecurity solutions is the most glaring and most damaging of all the epic fails in this book.

How long has value evaded *you*?

Do you find that so many technology companies have over-promised and under-delivered that **you've become conditioned to expect—and accept—failure?**

Do you think you have no better alternatives, that **you must settle for what you have and live with the ineffective products** and services offered to you?

With more than 4,000 security products to choose from, **do you throw your hands up in frustration and choose the easiest, or cheapest, or best-known product** you can find, even if you know you're not likely to get the results you need from it?

If you answered "yes" to any of these questions, we have just one thing to say:

LESSON #17

Value is limitless.

Entrepreneur Brian Evans notes that our brains are wired for us to fail—and they're too darn good at the job. He writes, "Part of the brain is literally designed to protect us with a fight-or-flight-type response. This and other brain responses make it almost impossible to be creative, positive, or even effective at what we actually want to do," [25] **making our quest for security value more or less doomed from the start—unless we change the way we think about and pursue it.** Here's how.

Step 1: Believe.
Nelson Mandela famously said, **"It always seems impossible until it is done,"** so start believing in the seemingly impossible—you'll be amazed at the successes that follow.

Step 2: Embrace Possibility Thinking.
Possibility thinking is the **willingness to see possibilities everywhere instead of seeing limitations;** it begins with viewing the world as open instead of closed.[26]

Step 3: Inundate Your Organization with Partners that Bring "Impossible" Results to Life.
Retrain your brain to cultivate and expect value and choose security providers that deliver transformational, rather than incremental, outcomes.

In other words, you can achieve value from all of your security investments—and you can continue to realize that value every day, week, and month, year after year, without settling, by retraining your brain to expect value rather than accept the same lackluster results you've been getting for years.

Retraining your brain will take conscious effort, but it's easier than you think. **Start by taking the expectations for excellence you demand in other areas of your life and applying them to your security investments:** When you buy a car, do you simply accept whatever the salesperson offers you, or do you

[25] Evans, Brian D. "Your Brain Wants You to Fail. Here's How to Stop It." Inc. November 15, 2016.
[26] Maxwell, John. "Possibility Thinking, Part One." John C. Maxwell. August 20, 2019.

ask for and expect the color, upgrades, and features you want? When you buy a house, do you take the spec home, or do you add options that improve the overall home environment for you and your family?

Your security spend can be approached the same way: **Ask for, expect, and believe you can receive the value you need.**

Of course, while you're working on becoming extraordinary and making the impossible possible, you can also quantify the investment return (ROI) on specific security tools based on the risk you want to reduce.

We'll use phishing attacks—one of the most widespread and insidious threat vectors—to demonstrate whether or not it makes sense to invest in employee training.[27]

Let's say you anticipate five phishing attacks per year at an estimated cost of $35,000 per successful attack; the cost to train employees to recognize and avoid a phishing email is $25,000. Here's how to calculate the ROI:

SECURITY RISK-REDUCTION ROI CALCULATION

ANNUALIZED RATE OF OCCURRENCE:	EXPECTED MONETARY LOSS FOR A SINGLE EVENT:	REDUCTION IN PROBABILITY OF RISK OCCURRENCE WITH THE IMPLEMENTED CONTROL:	COST OF CONTROL:
5	$35K	-85%	$25K

$148,750 = 5 × $35,000 × 0.85

- $148,750 — REDUCTION IN RISK
- 5 — ANNUALIZED RATE OF OCCURENCE
- $35,000 — EXPECTED MONETARY LOSS FOR A SINGLE EVENT
- 0.85 — REDUCTION IN PROBABILITY OF RISK OCCURANCE WITH THE IMPLEMENTED CONTROL

$$4.95 = \frac{(\$148{,}750 - \$25{,}000)}{\$25{,}000}$$

- 4.95 — ROI
- $148,750 — REDUCTION IN RISK '$'
- $25,000 — COST OF CONTROL (numerator)
- $25,000 — COST OF CONTROL (denominator)

4.95 × $25,000 = **$123,750**

SAVINGS PER YEAR

Investing $25,000 in employee training to reduce the risk of a successful phishing attack saves you nearly five times that amount annually and therefore provides tangible, quantifiable value to your business.

If a product cannot demonstrate quantifiably reduced risk levels to prove ROI, keep shopping. You're just wasting money if you continue to purchase tools that don't demonstrably lower your business risk.

Don't settle for flawed cybersecurity.

Don't believe you have to sacrifice security in order to achieve compliance success or any other business goal.

Don't give up. The right provider is out there. Impossible is possible.

There are amazing cybersecurity solutions out there, and they can be yours if you believe in what you once thought unachievable, adopt possibility thinking, and work with providers who do the same.

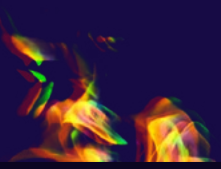
If you can make extraordinary a part of your everyday life and become accustomed to achieving, doing, and being incredible, then your brain will start to believe you and the value that has been just beyond your grasp will be yours at last.

CONCLUSION:

GET CYBERSECURITY CONFIDENCE TODAY

Now that you understand the eight epic cybersecurity fails, what's next?

We urge you not to forget the many lessons we've highlighted throughout this book. It's important to keep in mind that fear-based buying leads to poor solution choices; that product companies don't really care about your business objectives (and wouldn't keep profiting from failure if they were held to account); that compliance is the byproduct of good security—not the other way around; that without an ICARM approach you invite shelfware; that POCs must prove a business, not a technical, win; and that while there is no silver bullet in cyber, if you approach security investments with your business outcomes as the driver and if you invest in people, processes, and technologies, you will find no limitations on the value you can achieve.



THE MOST IMPORTANT CHECKLIST IN THIS BOOK

- ☑ **Define what business value means to your organization. If perceived product value speaks only to features or benefits and not to the goals of your business, you won't realize value from the investment. Make sure the solution works, that it's aligned to your business outcomes, and that it delivers the results you need.**
- ☑ **Switch from point-in-time engagements to continuous scanning, pen testing, assessments, remediation, management, and maintenance so you can achieve ongoing risk reduction and value.**
- ☑ **Challenge your vendors—all of your vendors—to deliver solutions with outcomes tied to your business strategy rather than their topline goals.**
- ☑ **Ensure your MSSP, if you have one, is committed to providing true remediation rather than creating more work by sending alerts you have to investigate and resolve.**
- ☑ **Use possibility thinking to guide you to alternatives that will enable you to realize extraordinary results and speed time to value regardless of where you are in your security journey.**
- ☑ **Ensure your security and business goals are aligned at all times.**

For many decades now, the marriage of people, process, and technology has been a proven best practice, but somehow this union has passed cybersecurity by. The industry has grown comfortable throwing technology over the wall and leaving it up to you to develop the processes and hire the people necessary to make it work.

It hasn't worked.

Armed with your checklist and a new way of thinking, you can achieve complete cyber confidence today—confidence that comes from keeping the faith and bringing together the tools, teams, and controls required to keep your security needs and your business outcomes in lockstep. Let us help you get started.

ABOUT CYVATAR

At Cyvatar, we understand—and object to—the ways the cybersecurity industry has failed. It's our mission to transform the way the industry builds, sells, and supports cyber solutions.

As the industry's first subscription-based, cybersecurity-as-a-service (CSaaS) company, it's our duty to empower our members to achieve successful outcomes by providing expert advisors, proven technologies, and a strategic process roadmap to guarantee results that map to business drivers, allowing you to succeed at security and:

- ☑ BENEFIT FROM EXCEPTIONAL CYBER TALENT
- ☑ COVER THE SECURITY BASICS
- ☑ ACHIEVE CONTINUOUS REMEDIATION
- ☑ AVOID SHELFWARE
- ☑ FORGO ACTIVITIES THAT WASTE YOUR TIME
- ☑ PROVE VALUE EVERY DAY

Our subscription-based CSaaS makes it easy for you to keep sensitive customer data and other confidential information safe, to feel confident in your security posture and compliance adherence, regardless of whether you're a security practitioner or not.

1 If you're in the early stages of launching a cyber strategy or lack the internal staff to build one for you, we offer subscription packages that deliver a fully managed security program for any size business.

The package includes expert practitioners, proven technologies, and a strategic long-term roadmap for a fixed monthly price. Subscriptions also cover incident response services; IT asset inventory; continuous vulnerability scanning; security gap analysis; and compliance services for standards including SOC 2, CMMC, NIST, ISO, HIPAA, HITRUST, and PCI.

2 If you have investments in point products but struggle to demonstrate efficacy and value from those tools, we offer comprehensive programs that link existing solutions with long-term strategic processes designed to provide business outcomes, continuous remediation, and ongoing solution maintenance.

Continuous vulnerability scanning and cyber management services ensure that once you achieve remediation you can preserve that solved state over time while maintaining all applicable compliance requirements.

3 If you're scaling quickly and require a complete cyber roadmap that can grow and scale with your business, we have a variety of programs that enables you to execute your security strategy at speed.

Our 100+ years of combined executive and CISO-level experience are at your service, providing top-tier recommendations and guidance and helping you to drive business growth while keeping your data and assets secure.

Not sure of next steps?

Hit us up and let us put you on the road to cyber confidence today.

START HERE → OR E-MAIL COREY & CRAIG →


CYVATAR.AI