HOW TO FAIL AT CYBERSECURITY

Inversion6

CONTENTS

SO YOU'VE DECIDED THE WEB ISN'T SO DANGEROUS

As a business owner and/or CEO you've likely been inundated with message after message about the importance of cybersecurity. It's enough to make you want to dig your heels in.

Government organizations continue laying down new compliance regulations that you're expected to follow. Insurance companies keep increasing (and changing!) their demands for you to acquire cyber insurance policies. You probably even have internal team members or IT professionals pointing out vulnerabilities and best practices to follow.

Oh sure, there's lots of evidence that supposedly points out the dangers of ignoring the threats present on the world wide web. The FBI's 2021 Internet Crime Report reported more than $6.9 billion in reported losses due to nearly 850,000 incidents of internet crime in that year alone[1]. Verizon's Data Base Investigations Report for 2022 cited a dramatic rise in ransomware attacks (up 13% or more than the previous five years combined) and increased focus (up 62%) on System Intrusion attacks on businesses supply chains[2].

All the experts and insight also show you're allegedly at MORE risk if you're a small or mid-sized business. According to the Department of Homeland Security, 50-75% of all ransomware attacks target SMBs[3]. According to the Verizon report, 37% of ransomware attacks targeted companies with fewer than 100 employees and 61% of all SMBs were targeted by some form of cyberattack in 2021.

It's just all...so much. You helped build your business. You know how it works and how it runs and you believe you know best how to keep it safe. You have a point to prove and by 'failing' at cybersecurity you can show it's all just a little over the top. You're firmly in the 95% of small business owners who are worried about things other than cybersecurity[4].

$6.9 BILLION
in reported losses

nearly
850,000 INCIDENTS
of internet crime

61% OF ALL SMBS
were targeted by some form of cyberattack in 2021

[1] https://www.fbi.gov/news/press-releases/press-releases/fbi-releases-the-internet-crime-complaint-center-2021-internet-crime-report

[2] https://www.verizon.com/business/resources/reports/dbir/?CMP=OOH_SMB_OTH_22222_MC_20200501_NA_NM20200079_00001

[3] https://abcnews.go.com/Politics/dhs-secretary-warns-ransomware-attacks-rise-targets-include/story?id=77512872

[4] https://www.cnbc.com/2022/05/21/americas-small-businesses-arent-ready-for-a-cyberattack.html

But not just anyone can fail at cybersecurity. It takes determination and a set of characteristics to create the conditions to make it possible.

Ignorance

They say it's bliss after all. If you don't go looking for a problem or assessing your environment, then it stands to reason you won't find one. Leave the hackers alone and they'll leave you alone, right?

Apathy

You have other, more pressing things to focus on. You're trying to grow or expand and simply don't care to rob those initiatives of momentum for a problem you think you'll never have to deal with.

Arrogance

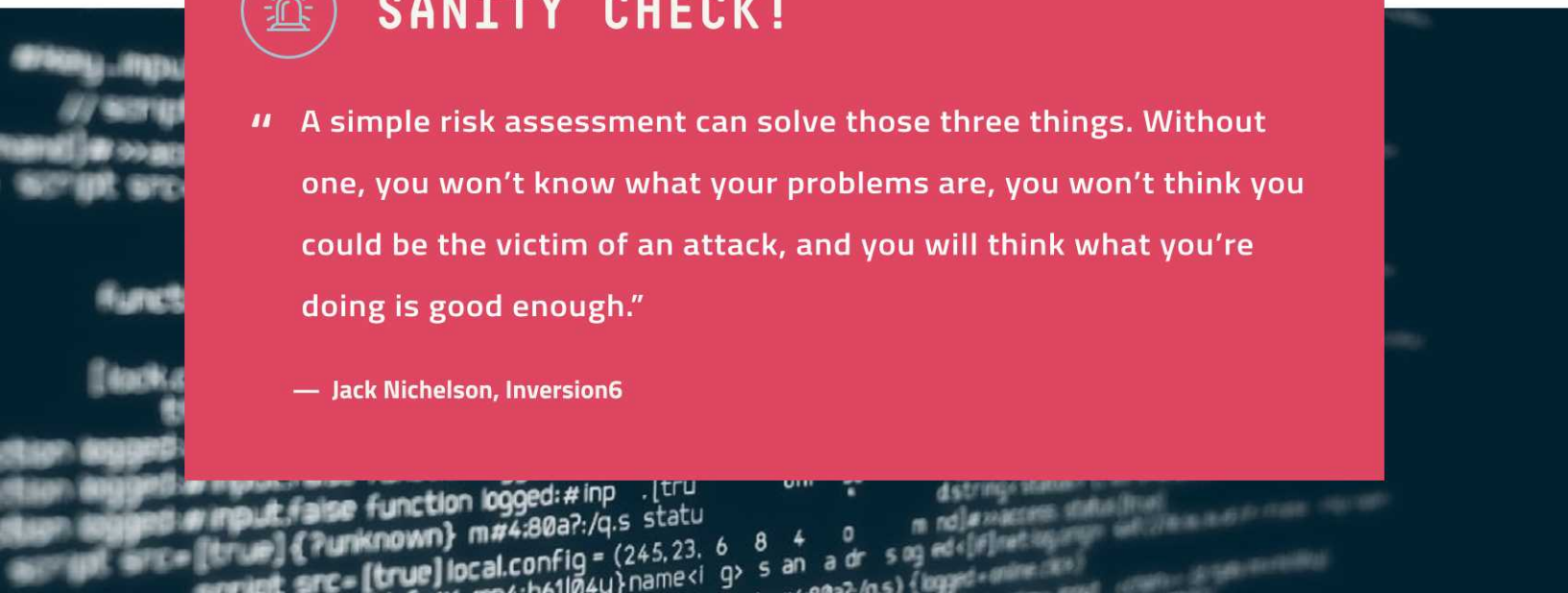
You've already dealt with cybersecurity. You got a firewall, some anti-virus software somewhere, right? You're golden. You've set it, now forget it.

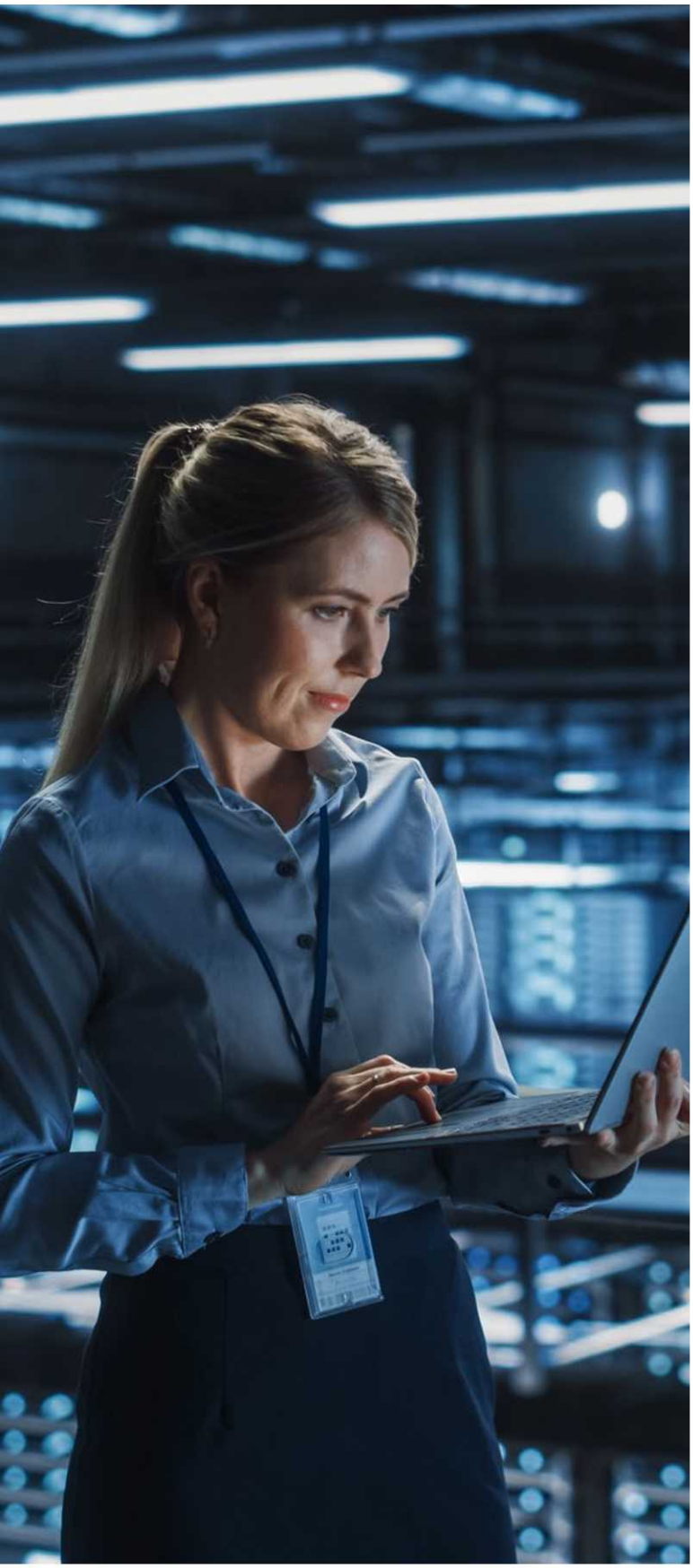
These traits represent a great start to failing at cybersecurity. But if you want to do so in truly spectacular fashion, there's more work to do (or, more accurately, not do). Let's go over five core concepts to keep in mind if you're determined to prove you're completely unconcerned with the business threats present in the interconnected world we live in.

At Inversion6, we take cybersecurity seriously. We know what it takes to provide the most secure environment possible and how most of the 'advice' presented here runs counter to what you SHOULD be doing. Our team of expert CISOs will offer counterpoints throughout.

SANITY CHECK!

> "A simple risk assessment can solve those three things. Without one, you won't know what your problems are, you won't think you could be the victim of an attack, and you will think what you're doing is good enough."
>
> — **Jack Nichelson, Inversion6**





THE BEST PLAN IS THE ONE YOU MAKE UP AS YOU GO

Strong foundational elements provide the best security, but you've always been a fly-by-the-seat-your-pants type.

If your goal is to fail impressively at securing your perimeter, digitally, it's important to discard everything you know about basic security hygiene. That includes NOT taking stock of WHAT you have and WHO has access. Lean into ignorance here — remember, curiosity killed the cat — and DO NOT plot out answers to simple inventory questions like:

- How many devices do you have on your network?
- What are the devices? Where are they?
- What software is installed?
- When were they last patched? How often are they patched?
- How many users have local admin rights?
- How many privileged accounts are in your environment?

Beyond scrapping assessments and discovery, striving to fail at cybersecurity means bucking all of the well-established basics as well.

Regular Patching — Your IT team calls it necessary, you call it tedious and unimportant! Sure, the US government's National Vulnerability Database (NVD) has more than 176,000 entries that regular patching helps address, but what's the rush?

176,000 ENTRIES
THAT REGULAR PATCHING HELPS ADDRESS

Password Management — Everyone hates changing passwords and the trial-and-error that follows after a recent switch. Well, never do it again. Keep one — the simpler the better — in perpetuity. Better yet, make sure employees share the same password!

ADDING MFA WAS EFFECTIVE IN PREVENTING
99.9% OF ALL
IDENTITY-BASED ATTACKS

Multi Factor Authentication (MFA) — Tying in a second method of authentication in addition to a password can be effective in locking up various elements, such as email. In fact, Microsoft found that adding MFA was effective in preventing 99.9% of all identity-based attacks. But who has the time to register their thumbprint or type in another five numbers in the name of security?

Identity & Access Management (IAM) — Securing your Active Directory properly, implementing password management and MFA, and more are all components of a strong and secure IAM policy framework. These are basic maintenance items that improve your security footprint. But, much like with maintenance on your home or car, they can be ignored without any repercussions whatsoever (maybe?).

SANITY CHECK!

" Running a network is like building a skyscraper. If your foundation is not structurally sound, you're just waiting to crumble."

— Todd Pigram, Inversion6

TESTING IS FOR SUCKERS!

Checking and rechecking security processes may be important, but you've got work to do.

IT and modern technology offer new paths to efficiency, optimization, and scalability. But your enthusiasm for these avenues is always tempered by caution from IT and security experts. For instance, it's strongly encouraged to analyze and test your policies and procedures at regular intervals to determine their integrity and how your business can respond if an incident or breach occurs.

While your competitor is 'testing' you'll take advantage by pushing the envelope on what the new software, devices, network, or cloud environment can actually, you know, DO. **You definitely don't want to invest in any of the following testing tools to improve your security profile.**

Risk Assessments

These address the inventory of your environment and help answer a lot of those upfront questions mentioned earlier. This tool is essential to discovering where you may be vulnerable and, with an outside perspective, considers things you may have taken for granted. Any plan built in a vacuum is not seeing the whole picture.

Data Recovery

Maybe you're backing up your data. But have you actually tested what to do if something bad happens? Have you tested recoverability, the process to gain the data (or access to it) in event of a ransomware attack? Maybe your backups are on the cloud, but your download capabilities are limited in practice. You could be trickling back data for weeks. Not all surprises are pleasant.

Incident Management

When a cybersecurity incident happens to your business, what do you do? Developing an Incident Response Management playbook alleviates the confusion and panic that accompanies cybercrime. Who do you call? Can you transact? How do you interact with your customers? Gaps in your plan can turn a bad situation into a potentially business-destroying one.

SANITY CHECK!

" We've heard so many times 'I should have done this or done that' in the middle of an incident response. Nobody wants to pay for it until they need it."

— **Todd Pigram, Inversion6**

WHO NEEDS METRICS WHEN YOU HAVE *INSTINCT?*

Relying on your gut has helped you get this far. Sometimes analytics just get in the way of bold leadership.

If you're doing your best to avoid testing your cybersecurity or running through tabletop exercises to gauge your responses, then you're already well on your way to checking off this next step. Information and data are the enemy if you're trying to fail at cybersecurity. Your approach is 'What I don't know can't hurt me' and by sidestepping gathering and noting KPIs, metrics, and analytics you've created a comfortable cocoon of obliviousness.

But beware, information can creep in and give you parameters to outline an effective security strategy if you're not careful. Remember when we noted that ignoring a complete inventory was the first step toward failure? That approach serves you well in metric analysis as well. You definitely should avoid answering (or even asking) these questions about your business security:

- What's the number of incidents your business has faced?
- How many vulnerabilities do you have?
- How fast is your team able to close those vulnerabilities?
- Where and how do you spend your security budget?
- Do you have a map of your environment and everything located in it?

log▪ging

Logging is actively recording the events occurring within your systems and networks. Each log entry should have information about a specific event.

mon▪i▪tor▪ing

Monitoring is the process of examining compiled logs to learn about application health, assist troubleshooting, find the cause of performance issues, and discover unauthorized activities.

Logging and Monitoring

Somewhere between incident response and analytics lies the logging and monitoring.

Of course, disabling any logging tools you have (so not even turning them on or configuring them) is important if failing to secure your network is your goal. You won't have any visibility into what individual users are on your network or what they're doing.

Alternatively, you could invest in logging technology of some sort and simply discard the other part of the equation. Logging will generate a ton of potentially actionable data, but without a monitoring solution in place to parse it, issue an alert, and so on, then it's 'empty' tech that is accomplishing little to safeguard your network. Either approach should be put on the fast track to failure.

SANITY CHECK!

> "Logging should provide who did what, when. It's often neglected, not thought of entirely, or misconfigured. Checking logs is often the first step in incident response."
>
> — **Christopher Prewitt, Inversion6**

IT'S THE INTERNET, JUST ACCEPT IT

This is all fine. Don't worry, be happy. Embrace the fun.

In a nutshell, cybersecurity is about risk mitigation. How diligent your business is in creating a security profile will directly relate to how much risk you're willing to take. If you're willing to roll the dice and trust the future of your business to the internet's good graces, there are several ways to show that through planning and implementation. Here are three examples:

1 We're Not A Target

You're not a globe-spanning, multi-billion dollar business, so why would some malicious actor halfway across the world take time to muck around in your infrastructure? 'We're too small to worry about this.' The idea runs counter to mountains of statistical evidence of course, and doesn't consider the simple fact that the smaller fish — those with fewer security tools, team members, and expertise — are the easiest to catch. Or, by working through a smaller, less defended company, hackers can work their way through supply chain and vendor relationships.

2 The Boss Calls the Shots

It's common for many organizations to craft a cybersecurity policy or process, and then make allowances for the CEO or other prominent executives to ignore them. Those at the top of the company hierarchy have many responsibilities, changing their password every six months shouldn't be among them. Again, it's one loophole; it's not like they are dedicated teams out there looking for this exact gap, right?

3 Convenience Trumps Security

The C-suite is often eager to unlock new capabilities brought on by technology and embrace the convenience promised by more interconnected systems and networks. But convenience and security are often at the opposite ends of the spectrum. IT is there to create value, through more efficiency, speed, data, and automation. Focus on that value, that convenience. As for the risk, figure that out when and if you need to. No big deal.

SANITY CHECK!

" The mistake is assuming you're too small, or too niche, or too whatever, that you're not going to get attacked, and that's simply not true."

— Chris Clymer, Inversion6

YOU'VE HIRED SMART PEOPLE, RIGHT?

Focus on your work, and let someone else worry about security.

If you're truly committed to failing at cybersecurity, you'll ignore the growing trend of criminals executing attacks that target people (for their credentials and access) versus going after application or system vulnerabilities. If you were concerned, you'd make sure that ongoing training on proper security functions and establishing a culture of personal responsibility were priorities.

Why should everyone play a part in securing your environment? You probably have an IT guy somewhere — I think his name was Scott — who is responsible for all that stuff anyway. Let them handle it.

With interconnected supply chains, hybrid and remote work setups, and vendor partnerships, cybercriminals are increasingly targeting individuals to gain a foothold and then expand. By educating your workforce and stressing the importance of individual responsibility your organization is preparing to face those threats with a unified front.

Reinforcing appropriate policies handling these situations, noting the importance of having home routers on the latest firmware, and offering tips on managing passwords can help secure your overall profile.

Communicating with the employees about the threat of Business Email Compromise and how social engineering attacks might appear could finally get them to quit clicking on every link that appears in a new email.

SANITY CHECK!

" It's hard to protect data when it's everywhere, which it is now. You have to build awareness and responsibility that everybody has a part in keeping a company secure."

— **Christopher Prewitt, Inversion6**

ABOUT INVERSION6

Inversion6 provides **customized security solutions to support your internal security efforts**. And while we've taken a light-hearted, tongue-in-cheek tone with the cybersecurity basics communicated here, we're serious partners dedicated to protecting your organization relentlessly — every hour of every day.

We provide a full suite of information security solutions that help define cyber security strategy and deploy it effectively.

- We conduct full risk assessments to find out exactly what the terrain looks like
- Our CISOs have extensive experience to map out plans and initiatives to address your specific environment
- We track new developments in technology and deliver that knowledge to you
- Most of our team has sat in the clients' chair before. We know the many pressures exerted on IT teams and their organizations

Inversion6 identifies your biggest risk areas, then offers methods to mitigate those risks. We bring a proactive mindset to the reactive world of cybersecurity.

We don't believe any company can afford to fail at cybersecurity. Connect with us today to start a conversation about how to ensure you don't.

Get in Touch with Inversion6

216.535.4100 | info@inversion6.com