Five Simple Signs You

Have Weak Cybersecurity

Ever wonder if your organization's cybersecurity systems are protecting you from being hacked?

Is the money you're investing in cybersecurity paying off? **Or have you just been lucky?**

Are you just dumping your money into a big cybersecurity bonfire?

In this report, you'll learn the five simple signs any CEO (and even CIOs or IT managers) can use to figure out if your organization is secure from hackers, crooks and internet thieves.

The following will probably shock you.

You may not like hearing it. But you'll have to admit it's true. These five signs will significantly impact all your organization's future growth and long-term success.

There are three types of organizations in this world when it comes to cybersecurity:

1. Those who are f**ocused and consistently improving** their cybersecurity
2. Those who **aren't doing anything** while watching other organizations lose everything because they've been hacked
3. The **victims** (although they aren't treated like victims): These are the organizations struggling to rebuild their reputations because they got hacked. These are the organizations who are being blamed, sued and/or fined for being unlucky enough to have a hacker break through their defenses.

No matter which of the three groups you currently fall into, one thing is certain:

You want your organization to be more secure.

DCS
DEALER CYBER SOLUTIONS

The problem is most CEOs don't know how to move up to higher cybersecurity levels (let alone the HIGHEST).

That's where we come in.

If you are already focused on security and constantly improving, we can show you how to improve your security posture and eliminate those blind spots.

If you run an organization that tends to stagnate when it comes to cybersecurity, we can give you and your team the push you need to make those improvements. Think of it like having a personal trainer or coach pushing harder than you'd push yourself during your workout.

Just by shifting your thinking and focus, your organization can quickly advance its cybersecurity at a rapid rate.

Finally, if you have someone who has a team that operates your cybersecurity **reactively or non-responsively**… OR you feel like they're more like a spectator up in the stands than a player making sure your data is secure… we can totally change (no, make that transform) their thinking, actions and capabilities.

If you want to transform your cybersecurity, you must make the move from mediocrity to greatness; that shift starts with doing the right thing with your user and client data.

We can help each type of organization we mentioned above to become proactive, focused and strategically thinking about cybersecurity.

We can turn security-focused organizations into out-performers, tackling the exact ways hackers are currently breaking into networks. We can turn greenhorns into security green berets AND we can turn security wallflowers into confident, capable and masterful security experts with a strategic focus on protecting what is important to your organization.

Plus, no matter which of the three categories you fall into now, **we can multiply your short and long-term accomplishments AND security success.** But it gets better:

We've concentrated our company mission around helping organizations protect themselves and leveraging points that your team might have overlooked.

But of all the breakthroughs we've uncovered — the five warning signs we cover in this book are the **clearest warning signs that your organization's cybersecurity is not only neglected, but at risk of a data breach, or even a reputation-shattering ransomware attack.** After nearly a thousand audits in 2021, we have found that these five warning signs are the best predictors of your security.

The five warning signs of an insecure network.

...that most CEOs fail to look at.

As a busy CEO, missing these warning signs is completely normal. They aren't things you'd ever think about unless someone brought them to your attention. However, they are extremely easy to identify if your organization falls into the subset of organizations at risk of an attack. Even the best businesses by all standard evaluations have fallen into the 'At Risk' category when it comes to network and data security simply because cybersecurity communication has felt unapproachable for such a long time. **Let's fix that now.**

Got a pencil?

Save this list somewhere you'll see it and review it AT LEAST once a month.

Consider attaching this list to the side of your monitor to keep it top of mind. Make certain YOUR organization can identify these security shortcomings by answering the following questions:

1. **Have you ever experienced a breach, ransomware or data loss?**
   Lightning never strikes twice, right? Wrong. In cybersecurity, hackers always come back to their victims. Why? Hackers identify their past victims as future targets. In their eyes, your organization is an easy mark. They already have a playbook from the first time they attacked you; why not come back and see if there are new opportunities? (Sometimes, they even leave backdoors to make the return visit even easier.)
   ○ **YES** ○ **NO**

2. **Can you login to your business email or network without an access token prompt on your phone?**
   Are you prompted for multifactor authentication when you access critical business assets? Hackers are constantly trying to bypass your security, and one of the best ways to do that is to get one of your team member's passwords. If you aren't being prompted for an access token when you log in with your password, not only is your data vulnerable, but your entire business is at risk.
   ○ **YES** ○ **NO**

3. **Is spam and unwanted email constantly appearing in your mailbox?**
   You probably already know that 91% of cyberattacks start with a phishing email. Did you know that 1 in 5 users click on phishing links? We both know that you'd never fall for a phishing attack, but what about one of your crazy-busy employees? Would someone else on your team click a malicious link?
   ○ **YES** ○ **NO**

4. **Are you getting lots of warning messages or popups?**
   Many businesses are just depending on antivirus to protect them, and guess what? Today, antivirus isn't enough. If you are seeing a bunch of pop-up messages or warning messages, you already have a problem. Chances are high that you've already been breached.
   ○ **YES** ○ **NO**

5. **Are you allowed to go to any website you choose with your work computer?**
   Have you ever been blocked when attempting to follow a link? Tricking users into clicking malicious links is the easiest way for an attacker to get into your network. Research has shown that 1 in 5 employees will click malicious links in email messages. Blocking those links is a critical component of an effective security program.
   ○ **YES** ○ **NO**

If you answered YES to any of the above questions, schedule a third-party assessment immediately.

Even if you answered NO to all the above questions, you aren't necessarily in the clear.

Here's the ultimate question: Are you **positive you don't have any blind spots or misconfigurations in your security tools?** Maybe your team is doing all right things when it comes to cybersecurity but how do you know for sure? Wouldn't it be great to have a qualified third-party review your cybersecurity and identify your weaknesses before a hacker does?

Here's how our confidential third-party cybersecurity assessments work:

1

We start by creating a custom link for your organization. We help you identify the people on your team who are the highest risk of being targeted or phished.

2

You have those people click the link.

3

Our team analyzes your security controls. We don't require passwords, administrative access or any changes to your network.

4

We provide you with an easy-to-understand report in under two business days. Our report provides steps your team can take to improve their security posture with clear instructions and explanations of the vulnerability.

How is a third-party assessment different than your team going over the settings in your environment and looking for vulnerabilities themselves?

One of the main challenges with cybersecurity is that it is **always changing.** What worked yesterday no longer works today.

This leaves many IT teams auditing against antiquated standards that no longer protect their networks. With a third-party cybersecurity analysis, you have an unbiased team of experts who focus on one thing: finding and exploiting vulnerabilities to help organizations like yours sleep better at night. Your team is trying to do the right things, the question is: what are the right things?

The biggest mistake people make with their cybersecurity is not getting started. Not taking the first step. So, what slows them down and keeps them from moving forward? Usually:

They think their data doesn't matter.

We hear this from victims of data breaches and ransomware attacks almost every time. When we've gone through security audits or assessments, many well-intentioned businesspeople tend to tell us that their data isn't worth anything and that it doesn't matter. The problem is, you're probably not thinking about your data in the right context.

Once, our security team ran into an issue when they were dealing with a small publisher. They, perhaps like you, thought their data wasn't worth much to them.

But one Monday, the office manager's email account was compromised. The attackers exploited that single email account to trick her team into sending them $40,000. Basically, her team wired payroll to the wrong account.

Can you imagine being the person responsible for wiring your entire payroll to the wrong place?

Think about the folks that didn't get paid on time. Because it was a business account, they couldn't get their money back; many banks do not take responsibility for money wired to the wrong account.

Do you ever wire money?

Do you have any employee information or personal information on your systems that could be used to perform identity theft? Could this information be used to submit fraudulent tax returns?

They believe cyber insurance will cover it.

A few questions here…

Does your cyber insurance cover reputational impact? Will they pay you extra for the impact a breach is going to have on the relationships you have with your clients?

Just because you have insurance doesn't mean you want to use it, right?

I'm sure you have health insurance, right? But you don't take unnecessary risks with your health.

Just because you have health insurance doesn't mean you want to experience open heart surgery you don't need.

So, even if your cyber insurance company paid for all the recovery costs, would you still be willing to go through an event where your entire computers systems were offline for a week? What about a month? **Typically, ransomware events cause 21 days of lost productivity, even when the data can be restored.**

What if your clients are contacted by the attackers? What if attackers send emails containing malicious files to your clients pretending to be you?

Your cyber insurance company will cover your data cleanup, but what about the experience your clients go through when they find out some attacker had been posing as you?

We know the type of devastation this type of event causes to your team, your clients and even your vendors. Even with cyber insurance, you don't want to experience a network breach or ransomware.

They assume their current IT team already handles security.

Hackers are constantly coming up with new tricks.

They spend 100% of their time focused on breaking into networks.

Does your IT team spend 100% of their time thinking about protecting your network? Or are they splitting their time between server migrations, end user support and compliance?

We spend 100% of our time coming up with ways to get past security tools. We don't support users and we don't do projects. What you get from us is a second opinion from a specialist.

If your family doctor recommended heart surgery, you probably want to get a second opinion from a cardiologist, right? You wouldn't go to another family doctor or general practitioner for that second option.

Why wouldn't you want to get a second opinion from a specialist on something as important as your business data and reputation?

They think they're fine because no one's hacked in yet.

Obviously, if you haven't been hacked yet, you haven't gone through the pain.

You haven't experienced the embarrassment. You haven't had clients and employees upset with you. You haven't had to talk to the press. You haven't had to negotiate with a hacker. You don't know what it's like to be hacked.

In the business community, we've seen a huge increase in hacking activity, specifically ransomware. Why is ransomware increasing exponentially every year? There are a few factors at play:

1. For the past 4 years and counting, there've been more vulnerabilities in software, operating systems and firmware (the software that runs on devices like internet-connected cameras and thermostats).
2. Computer systems are becoming more complicated, making it difficult for people tasked with defending these systems to identify malicious activity.
3. Hackers have pressure to act now. Think of it like the fear of missing out you experience when there's a sale or a very short-term offer. If you were a ransomware gang, you'd want to get this done while the getting's good, right?

All these factors lead to an increase in malicious behavior AND an increase in the number of successful hacking events. This leads to more money going to ransomware gangs which then funds them to invest more time and effort into hacking. As the cycle continues, the number of victims continues to rise, and so do your chances of getting breached.

They believe they are secure because they are compliant.

Being secure and being compliant are two different things.

This is like the difference between following the law and being safe. It's almost like wearing a seatbelt; it's the law.If the car catches fire while driving, the seatbelt won't keep me safe.

One time, a hospital engaged the team to assist with forensics and ransomware recovery. But two months before said attack, the hospital completed a full HIPAA Risk Assessment. Even though the Risk Assessment came back covered with green dots and accolades about their compliance to the HIPAA standards, every single computer on the network was impacted.

It took over 20 days to recover their environment, even though they are doing all the right things according to standards outlined in HIPAA.

The bottom line is simple: being secure is different than being compliant.

They think they'll just pay the ransom.

Even in the best-case scenario, paying the ransom will put you in a spot where your systems are offline for a couple of days, if not longer.

Also, when you pay the ransom, there's only an 80% chance that you'll get your data back. Would you pay $40,000 to hire an employee or contractor that only had an 80% chance of performing? Heck no!

When you pay a ransom, remember you're dealing with criminals. They often end up asking for more money; the question you may be posed after making your first payment could be "hey, you paid us the $40,000… how about another $20,000, if you really want your data?"

Plus, what if there's a bug in the ransomware? What happens if the attacker wants to do the right thing, they give you the code to release your data, and it doesn't work as expected?

Lightning never strikes the exact same spot twice. Hackers on the other hand, do.

They think their backups will save them.

Today, backups aren't very effective against ransomware attacks.

That doesn't mean you can get away with not having backups. It just means that, as a ransomware response strategy, backups are not the solution.

Hackers will exfiltrate data for sale or use it to contact your clients and shame you into paying a ransom. They basically blackmail you into paying them to be quiet and leave you and your clients alone.

Hackers are GREAT at finding and destroying backups.

We've watched major events happen to IT businesses like Garmin, who had to pay the ransom to get their servers back online. Do you think that they had backups?

You bet they did.

Hackers are often in the network for a long time without being detected. During this time, they hunt backups, look for data of interest and figure out how much your organization would be able to spend on a recovery without just going out of business.

They think because they are in the cloud, they are safe.

How do you access data in the cloud?
Do you use your computer? Your phone? Do you have a tablet?

Cloud providers are not responsible for the devices you are using to access your cloud data.

And if an attacker gets to your computer, they're going to have access to your data in the cloud. They may be even able to abuse your privileges and delete the data. Worse, they might be able to extort money from your clients, your other vendors, or even create fraudulent transactions.

This is why just being in the cloud isn't good enough to protect your organization from hackers. You will need a strategy for protecting the devices that are accessing your cloud infrastructure as well.

They think they're too small to be hacked.

Why bother hacking you?

The media is doing smaller organizations a tremendous disservice when it comes to cybersecurity. They focus on big organizations. They share stories of universities, governments and huge organizations being hacked. They don't share stories about the two-person law firm who had to pay $80,000 dollars from one of the partner's personal retirement

accounts to make sure all his client data didn't get shared across the internet. They don't share the story of hackers blackmailing a prominent couple in middle America with transcripts from a three-year-old deposition (which the couple believed to be private) that included every detail of the husband's affair. A private discussion they'd worked out and put behind them was now being used to threaten their reputation.

The bottom line is that small organizations get hacked all the time.

They just never make the news.

The benefits of third-party assessments are obvious.

You'll get assurance from an outside source that your team is taking the right steps to secure your organization. Everyone is focused on doing a great job and we all want to do the right thing. Having a third-party assessment provides a new perspective on your cybersecurity. Our team will show you exactly what the hackers will see when someone on your team clicks a malicious link.

Easy-to-understand results.
Our reports are designed to clearly and easily communicate risks to your organization. You'll learn how easy it is for hackers to get to your information when it isn't properly protected and make sure your team is adhering to good cyber hygiene. We will likely identify information you've long forgotten even exists.

Measure where your cybersecurity is today. We'll examine your data encryption and discover what a hacker can access within an infected device to determine if your network would withstand an attack.

Get clear steps to address issues with the team and tools you already have. Our framework is vendor agnostic. Start addressing security issues with the team you have and the resources you are already investing in, without having to switch anything!

Prioritization of the most important vulnerabilities to focus your efforts. Until you see where your data security problems lie, you won't know where to focus your team's energy. We will validate where your security controls are working as expected and where they aren't in order to help your team prioritize what will have the most impact.

Reducing your risk of growing attacks. Cyberattacks are not going away and until your team and leadership are able to understand the issues and relate them back to your network, you'll never know how secure your data really is. It doesn't matter whether you have worked with the same IT team for years; the threat landscape is changing so quickly, it's hard for even competent teams to keep track of everything. A third-party assessment is exactly what businesses need today.

The bottom line: no one knows what they don't know unless they take the time to learn. No matter where you are starting from, a third-party cybersecurity analysis identifies the path forward.

DCS
DEALER CYBER SOLUTIONS