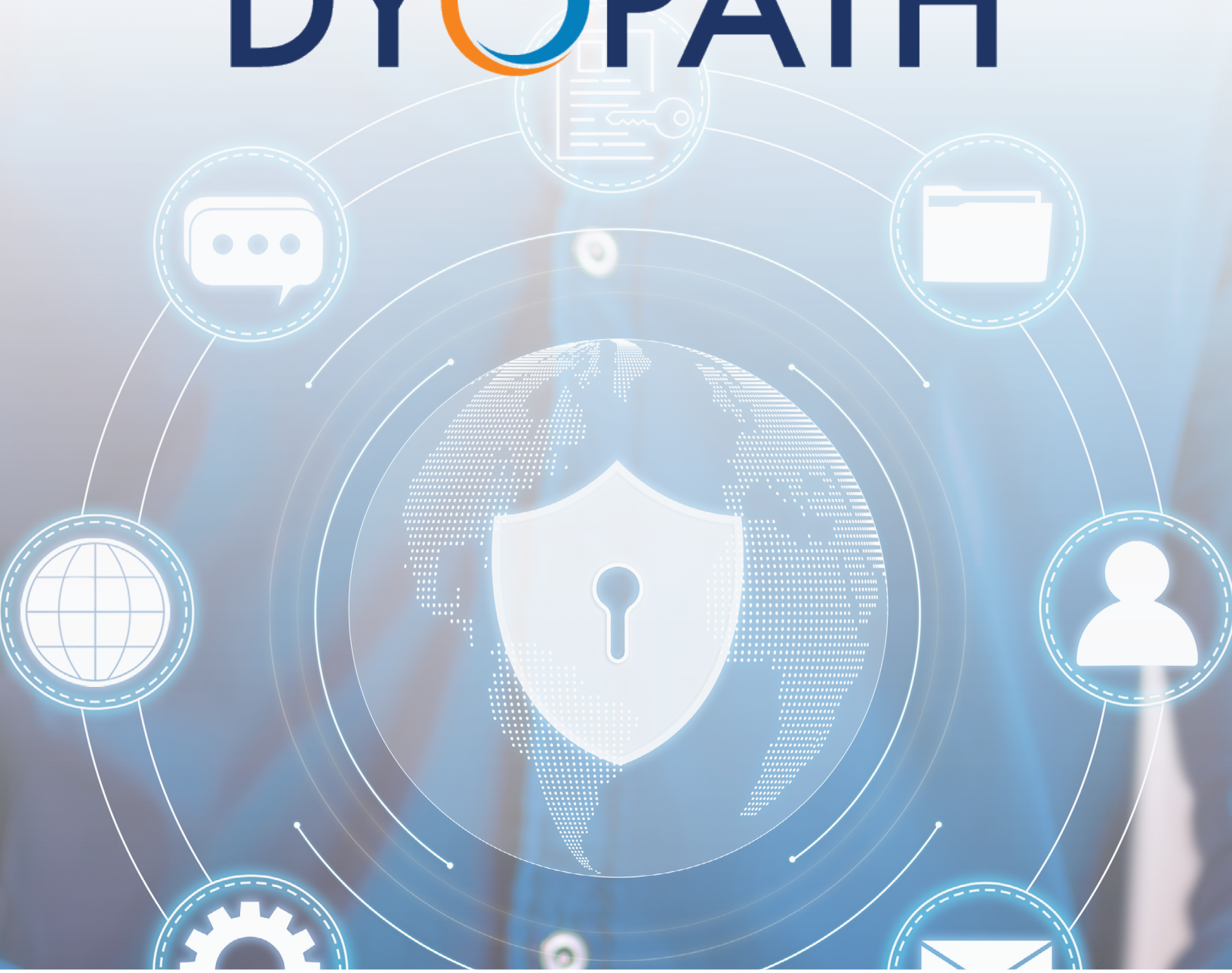
DYOPATH



THE SMB BATTLEGROUND:

CYBERSECURITY STRATEGIES FOR SMALL & MEDIUM BUSINESSES

Cybersecurity is a great equalizer. Cybercrime affects the biggest, richest companies in the world — and it also affects small teams and solo entrepreneurs. This is a problem because while smaller companies have many of the same exposures and risks as their much bigger counterparts, they have far smaller budgets and fewer resources to defend themselves.

Additionally, many small and medium-sized businesses (SMBs) are unaware of the magnitude and number of threats they face. Even those that think they have advanced, robust security processes in place often have glaring gaps in their defenses.

In this white paper, we'll draw on insights from Jeffrey Whitman, Cyber Risk Strategist at Black Kite, who has advised tens of thousands of security and risk leaders around the world, and Sam Bourgeois, Director of Cybersecurity Services at DYOPATH. We'll also call attention to the risks facing SMBs right now and talk about the best strategies organizations can put in place to remain safe.

A Lack of Confidence in Security

One of the biggest issues in cybersecurity right now — that both Jeffrey and Sam have noticed — is a glaring lack of confidence from businesses of all shapes and sizes. Many companies feel strongly that their security isn't where it needs to be. What's more, those that do feel confident are often simply unaware of the risk and become less confident when confronted with the reality facing them.

Jeffrey says, "We see all these new vulnerabilities — all these exposures in our digital and physical supply chains — and I think especially midsize enterprises and small businesses have maybe even greater exposures and fewer resources to throw at this problem."

Further, many companies are still failing to implement ongoing monitoring. They treat cybersecurity as a series of separate responses to problems as they arise, but this approach is not sufficient. There's a better way to manage cybersecurity.

Building Resilience

In the context of cybersecurity, resilient businesses are able to maintain a minimum level of viability no matter what happens. Jeffrey says, "A lot of people [...] think about, 'What happens if our building collapses or the data center falls into a sinkhole?', but it's so much more than that. It's what happens if a file gets deleted by mistake. What happens if during a terrible storm, a key person can't get involved?"

Resilient businesses, then, are the ones that can keep their operations up and running even in the midst of a data breach, or a natural disaster, even if they do so imperfectly.

Resilience goes beyond your security team. Company executives and stakeholders care deeply about resilience because they are invested in business continuity at all costs. Good security teams must be able to show leadership that the business is capable of surviving crises.

From a supply chain perspective, resilience means making sure your business has all the components, services, and infrastructure to keep doing its job and serving its customers at all times. The COVID-19 pandemic shined a light on many organizations that were unprepared here — many businesses ground to a halt for weeks at a time due to a shortage of specific parts.

Don't Lose Sight of the Fundamentals

How can small businesses build a resilient, effective security infrastructure that stands the test of time?

It's easy to think the answer lies in sensational trends and emerging technologies. Everywhere we look, there are new, terrifying threats to focus on — AI, deepfakes, ransomware-as-a-service, and so on. There are also new cutting-edge security tools and techniques to defend against these dangers, all of which are extremely important, relevant, and worthy of your attention.

But in this quagmire of trends and headlines, you must not lose sight of the fundamentals of cybersecurity. Deepfake technology, for example, is a very serious threat, and there are lots of promising new tools and techniques to defend against it. But the best defense against deepfakes is strong fundamentals: phishing awareness, phishing simulation, and phishing filtering.

Jeffrey talks about the dangers of getting caught up in "top-of-funnel" security activities and losing sight of the most important things — business impact and business operations. He says, "Your businesses care about three things: money coming in, money going out, and if something goes bad, who's in trouble?"

Having strong, reliable policies and governance is even more important for smaller organizations that don't have the budget to buy every new, cutting-edge tool as soon as it's released. SMBs need to be on point with the basics:

- Is your data protected?
- Are your systems protected?
- Are your operations stable?
- Did you invest in an appropriate way — in line with your risk appetite and tolerance — to protect your business?

Jeffrey says, "I think most people aren't even doing those basic things. Instead, they're moving to these cool distractions, and they're great, but they keep you from doing the basic stuff, which we need to do, and they're still not getting done. We're still not getting our systems patched. And that is true for big companies as well as small."

Sophisticated, specialized, emerging security tools are incredible. But they're only valuable if used on top of strong policies, procedures, and governance.

3 Major Challenges for Managing Risk

When it comes to managing the risk in digital ecosystems and protecting supply chains, there are three main challenges that small businesses (and most businesses) have to contend with.

Who Are You Dependent On?

Given how interconnected the economy — and in particular, the digital world — is today, your security is always going to be heavily dependent on the other entities and organizations you work with. This means your suppliers, partners, cloud vendors, software integrations, and much more.

You can't just go to Google or Amazon and ask them to improve their security, so this element of cybersecurity is always outside your control. But worse than that, many companies aren't even aware of who is in their ecosystem and suffer from a serious lack of visibility into the threats around them.

One example of this took place in early 2024, when the Snowflake cloud platform came under a wave of attacks. Hundreds of vendors were impacted, but many were completely unaware they'd been affected, or even that they were associated with Snowflake.

How Do You Know Who You Can Trust?

Reliable cybersecurity depends on accurate, honest data from many different sources. Some of these you can control directly, like the data you glean from monitoring your network. But other sources — like questionnaires from employees or partners — are less clear-cut.

How do you know that you can trust the people you're working with? It isn't that people are intentionally dishonest with what they report; they may simply be unaware.

Point-in-Time vs. Ongoing

Security in today's world has to be an ongoing, relentless process. Unfortunately, many organizations rely too much on point-in-time snapshots — consciously seeking out information when, for example, onboarding new partners or updating contracts.

But this process of gaining visibility should always be taking place. Companies need to figure out how to take in all the relevant security data and intelligence and use it to fuel better, more accurate decision-making.

Is There a Lack of Cohesion in Cybersecurity?

"I had this epiphany last year that we're at war," says Jeffrey, "And we are losing, in no small part, because we are a fractured set of defenders, and the attackers are unified."

This lack of unity both between and within companies is an enormous problem for security. Successfully defending against the myriad of present-day threats is only possible if security teams communicate effectively and constantly with their other internal teams, and with the security staff at other companies.

Multiple companies are being hit with ransomware attacks multiple times, from multiple different gangs, and the frequency of these attacks is skyrocketing. This is happening because the bad actors are collaborating, too.

So how do companies work together, without exposing their intellectual property to their competitors? Standard questionnaires, standard repositories of shared knowledge, and centralized places to collaborate are all good places to start. And this needs to happen soon. Companies need to put aside some of their natural inclination to compete and work with others in their industry to remain safe.

Solving the CISO Communication Problem

Cybersecurity has a communication problem. While many chief information security officers (CISOs) think of themselves as good communicators, executives tend to disagree.

One major reason for this is a lack of focus on concrete business impact when discussing security issues. When CISOs need funding or support to improve security and solve problems, they will often make the case to decision-makers from a security perspective.

Instead of highlighting what the business stands to lose in the event of an attack — in terms of finances, reputation, and legal consequences — CISOs often frame their cases in security-specific language that executives don't understand.

But CISOs and their teams need to instead learn to speak the same language as company executives and stakeholders. Sam says, "Dig through all the log material and trend data and threat reports, and then convert that into human speech. Here's what your business impact is." In other words, come prepared with statistics and data and show clearly what the business stands to gain from cybersecurity.

The Power of Trustworthy Data

The solution to building a safer, more security-conscious small business rests on having access to highly trustworthy, high-quality data. Trusted sources are important because of the huge (and growing) amount of misinformation out there. The rise of AI and deepfakes has meant a proliferation of unreliable, often intentionally misleading, information.

On top of that, the nature of the internet and social media means a large number of articles and posts around a single, hard-to-find original claim are typically inaccurate. When making decisions, you need to rely on solid, trustworthy, and (ideally) multiple sources.

According to Sam, "If your cybersecurity program, in any business of any size, is not data-informed by your market, your industry, your geography, your personnel — you're starting with fallacies, you're starting with misinformation, you're starting with bad data."

On the other hand, when you use reliable sources, your decisions will be based on high-quality data. You'll be able to make security decisions more confidently and avoid being misled by disinformation from malicious sources.

Secure Your Business With Black Kite & DYOPATH

According to Jeffrey, "Data is ones and zeros. Information is what you get when you analyze those ones and zeros and apply a business context." Getting clear on what your business and your executives really care about will allow you to collect timely, relevant data that you can rely on to solve your problems and make informed decisions around risk.

This is where Black Kite and DYOPATH can help. DYOPATH's well-honed process-based mechanism for managing security infrastructure combines with Black Kite's intelligence to help clients make better and more defensible decisions to secure their organizations and comply with all relevant laws.

Black Kite's approach to intelligence digs deeper than surface-level sources to help companies gain insights into their third-party vendors and the risks associated with them.

If small businesses want to defend themselves against cybercriminals and survive, they need to stay ahead of the bad guys by constantly monitoring and assessing their vulnerabilities, using reliable data, and staying vigilant at all times.

To learn more about DYOPATH's partnership with Black Kite and how we can help you build a more robust and resilient small business, schedule a call.

If you want to learn more . . .


Visit our Website


Call us at (866) 609 - PATH


Email us at solutions@dyopath.com