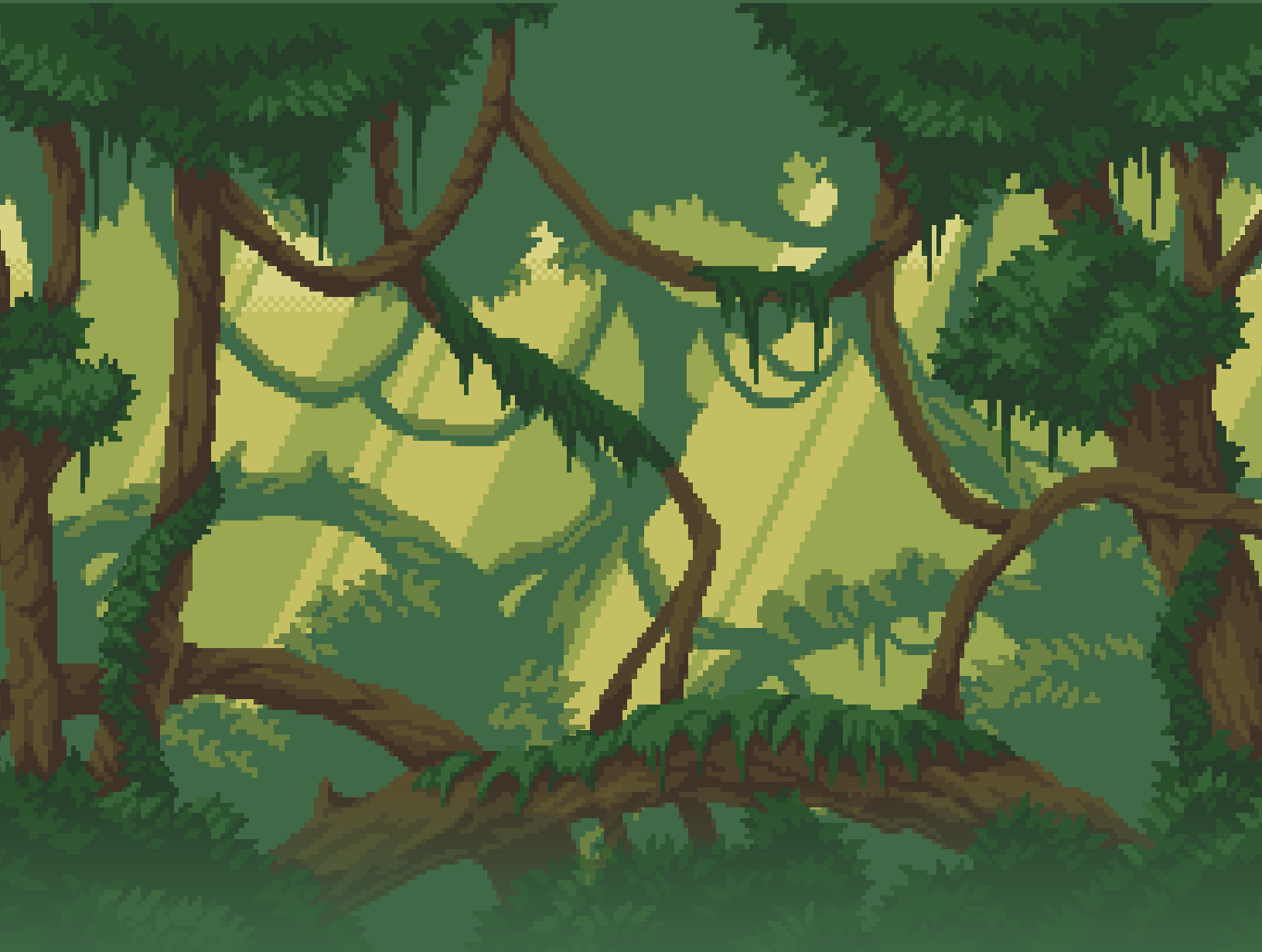


DISPELLING THE ILLUSION OF SECURITY

YOUR MAP TOWARD RESILIENCY IN THE DIGITAL JUNGLE

spriteCloud
Cybersecurity

PART 1: MANAGING THE PITFALLS OF THE DIGITAL WORLD

Do you remember Pitfall, one of the most successful video games of the 80's? In under twenty minutes, Harry had to find the 32 treasures hidden in 250 different screens in a pixelated jungle, while avoiding the various traps and hazards that lie in the way. Achieving digital resilience in today's interconnected digital world feels very similar to successfully avoiding the pitfalls of that jungle and winning the game.

Technology has changed a lot since the 80's, and for those who can navigate the digital jungle, opportunities abound. However the traps and hazards – such as phishing and ransomware – have grown just as much as the opportunities. In 2019, the monetary damages caused by cybercrime amounted to $3.5 billion globally, with businesses becoming the primary target for ransomware attacks.

What's more, those pitfalls are constantly shifting and don't resemble those of the analogue brick and mortar world. In the digital world, you must run just to stay in place.

Most business leaders don't have the time to keep up with the ever-changing map of digital pitfalls and are at great risk of operating under an illusion of security. That illusion could cost businesses more than they can afford, as 60% of SMEs who faced a cyberattack shut down within 6 months as a result.

Making the right call on cybersecurity is one of the most important business decisions you can make, particularly if your business generates a significant amount of revenue from digital assets or as your business moves to the cloud. However cybersecurity is not a simple yes or no decision. If you take a wrong step, and you could alienate your customers, damage your reputation, or face heavy fines and legal charges.

Yet an overly cautious approach may be just as dangerous. Bury your staff under excessive security protocols and they may no longer be able to perform. Or worse, they may bypass the protocols for convenience, leaving you exposed and unaware. Overwhelm your customers with too much security, and they might well run to the first competitor offering them a more convenient experience.

However, as seasoned business leaders know, in risk lies opportunity.

Building a resilient cybersecurity strategy is the best way to navigate the digital world and make the most of the opportunities it holds. Such a strategy can serve as a training ground for your team, and be the bedrock of a dynamic company culture. It can be the lynchpin of your customer engagement strategy. It can be the place where you find yourself; as a leader, as a business and as a team. It provide a strategic opportunity to define where your core value resides, satisfy your customers and gain market prominence.

This paper's goal is to provide an impetus for developing a resilient cybersecurity strategy within your business. As you continue reading about how a cyber resilience package is built, you will be armed with a game plan to address your business' perspective on cybersecurity. Cybersecurity can no longer be an afterthought, it must be as core to your business as its product, services, and vision.

Replacing the illusion of security with confident risk awareness requires a change of culture. Your cybersecurity systems depend on more than machines: breaches are mostly caused by human error. Building a resilient cybersecurity strategy requires expert guidance and training.

PART 2: A CYBER RESILIENCE PACKAGE FOR THE DIGITAL WORLD

When it comes to cybersecurity, there are two paths you can take to navigate your business through the "jungle" that is our digital world.

One is to go at it on your own, by assuming you know enough to plot your own cyber resilience strategy and rely on tools that are not purpose-built for the journey. On this path, you lay the responsibility of your security on your service and software providers, assuming their priorities are the same as yours. Just like a pile of leaves could hide a pitfall, this creates an illusion of security for your business.

The other path is to choose a company to guide you and your business to building a strategy using the right tools, and to develop the skills to continue on your own.

At spriteCloud, we are cyber security experts. We will guide you through the processes and tools, as well as help you build confidence through better understanding. We will dispel the illusion of security and help you understand that there is no such thing as zero risk, only strategies to reduce it to an acceptable level.

spriteCloud works as advisors to experienced C-suite executives and business leaders in European Small and Medium Enterprise (SMEs), organisations where digital expansion is essential but not a core competency.

We will help you to test your existing systems, or support you when you upgrade them, move to the cloud, and develop new products and services. We also accompany you during more fundamental digital transformation, whether you're going mobile or embracing new hardware.

We work with your people to build a cyber resilient culture, focusing on the following areas:

RISK AWARENESS

We help your team build deep awareness of cybersecurity risk. We train your people to develop common mental models and a common vocabulary to discuss those risks. We do this from the boardroom to the workers' floor, and treat them both seriously and realistically.

PROCEDURE DEVELOPMENT

We develop procedures that your people can follow, from the perspective that increased compliance reduces risk.

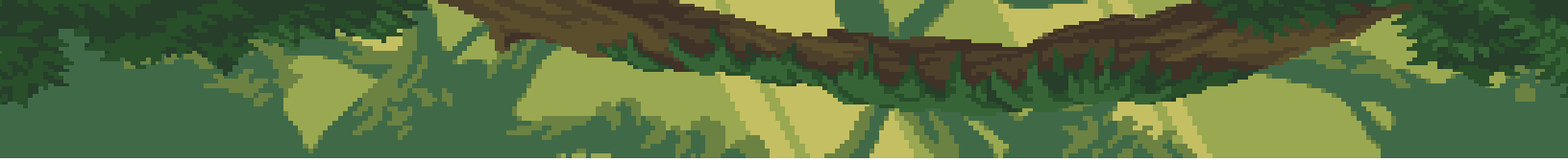
ENCOURAGE AN OPEN CULTURE

We encourage a culture of openness. By getting rid of unfounded fears and taboos, we create conditions to quickly spot weak points, human failures and threats before the consequences have a chance to negatively affect the business.

AWARENESS OF ECOSYSTEMS

We embed a solid, customer-focused cybersecurity model in all your interactions with customers and suppliers, to protect your business and theirs.

Cyber resilience is invariably connected to our technology. It is therefore important to understand how to implement a cyber resilience strategy from a technical and process perspective. spriteCloud guides your path to digital resilience with our four primary directives: appraise, test, recover, respond.



1. APPRAISE

We help you figure out what assets are most valuable to you. How can you seize the best opportunities and avoid the pitfalls, if you don't understand what's important in the first place? We run executive briefings and workshops to dispel the illusion of security by helping you identify your business's risk appetite (i.e. defining the acceptable level of risk).

- Through security awareness training, we help you understand the basics of cybersecurity: what matters and why.
- We help figure out the relative value of your business assets, and which you most want to protect. We do this based on a business impact analysis of your company assets.
- Through a security assessment, we help you figure out which of your business assets are exposed to risk – assessing the likelihood and impact of each risk – to establish your current risk profile.

2. TEST

We look for vulnerabilities in your systems and assess risk appetite alignment. spriteCloud specialises in vulnerability scanning and penetration testing, which are activities carried out by our 'ethical hackers.'

- We offer a diagnostic service, where skilled cybersecurity experts assess your key vulnerabilities, and measure them against your risk appetite.
- We will use industry leading tools to scan for vulnerabilities in your system that need patching.
- We offer more advanced services, including:
  Quality assurance: we work with you to establish best practice across your systems.
  Defence upgrade: we check whether your system is up-to-date with latest fixes and patches.

3. RECOVER

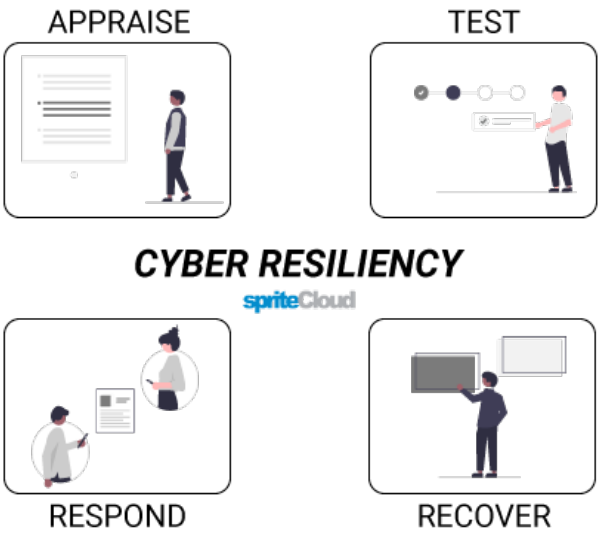
We help you bounce back after a crisis. In the digital world, there is no such thing as zero risk. Rather, what matters is to manage risk so that the businesses can recover quickly from a failure. For this, we offer services that extend beyond technological fixes.

- Incident response and recovery: after an incident or a breach to your systems, we work with you to assess the cause of the incident and the extent of damage, and help you return your systems to a more secure state.
- We work with your team to identify vulnerabilities and remediate them. In particular, we help you review your procedures, policies, and cybersecurity culture to reduce the risk of human error.

4. RESPOND

We work with you on building a whole-of-system cyber-resilient culture. Navigating the digital world is taking a journey into the unknown, where your safety is not as certain as in the physical world. That is because technology evolves at high speed, constantly transforming the risk landscape.

- Each piece of hardware, software or cloud application may be perfectly safe in itself, but their points of connection are where security gaps exist.
- Your business is closely connected with others. If the security systems of your client or suppliers are breached, yours may be exposed. Or even if your systems are safe, their failure may cause you serious business-continuity problems.
- Cybercriminals come in many forms. Some are cyber terrorists seeking to destabilise regimes. Some are part of cyber warfare where businesses are collateral damage. Many are individuals or crime groups seeking a quick payout by targeting businesses for ransom.



This level of interconnection is why the digital world offers so many opportunities, but also why it carries such a high level of unpredictability. With our help we can help your business maximise the opportunities of the digital world while mitigating the dangers it presents. Take a moment to think critically about how your business would handle a cyberattack.

- How would your business deal with its systems being locked down and held ransom by a hacker?
- What processes are in place to ensure people can't impersonate key decision makers?
- How do you prevent someone with access to one system from threatening the integrity of other systems?

If the thought of such scenarios makes your start to feel uneasy, it's because you now fully understand the weight of the problem. Forunately, the solutions to these problems are available and we can help.

***

Talk to spriteCloud about removing the mysteries of the digital world and dispelling the illusion of security by creating a resilient cybersecurity strategy for your business. Get in touch with us for more information or to learn about how we can support your business.

Contact spriteCloud

spriteCloud Website

Penetration Testing Services

Vulnerability Scan Services

Security Awarness Training

Cybersecurity Articles