# Cybersecurity on a Startup Budget

A founder’s practical guide to securing the business

Barnaby Grosvenor



Sponsored by Cygienic.com

# Preface

## The Author

Barnaby Grosvenor is a seasoned Global Chief Information Security Officer with over 30 years of experience in cybersecurity, risk management, and digital transformation. He has advised boards and executive teams, building resilient security programs for Fortune 500 companies, financial institutions, and startups. A trusted industry voice and a founder himself, Barnaby brings deep enterprise expertise into the startup world.

## Why this book - and how it will help

A practical guide for non-technical founders

This handbook is written specifically for founders, operators, and early employees who don't have a technical background but are still responsible for protecting their company. You don't need to become a security expert; you just need to understand the risks that matter and the actions that reduce them.

## A simplified, no-jargon approach to cybersecurity

Cybersecurity can feel overwhelming, expensive, and full of confusing terminology. This guide strips it back to the essentials, focusing on clear explanations, real-world examples, and practical steps you can take immediately, even with limited time, money, and expertise.

## From zero to hero: building a realistic security foundation

We'll take you from having little or no formal cybersecurity in place to running a structured, defensible program. You'll learn how to assess risk, define priorities, create a basic security strategy, set realistic budgets, and put a plan in place to reduce your exposure as your startup grows.

## Built for startups operating on tight budgets

Every recommendation in this guide is shaped by startup realities: limited cash, small teams, fast growth, and constant trade-offs. We focus on high-impact, low-cost controls and help you avoid over-engineering or spending money where it doesn't add real value

# Chapter 1. The Risks are Real

You've done the hard work of building the business. Congratulations. Now comes the part many founders underestimate - securing it.

Imagine waking up to find your business wiped out by a cyberattack - no access, no clients, no way back. It's exactly what hit Mt Gox, Travel Ex and Medic Secure, to name but a few.  Many Startups simply never recover from the downtime, loss revenue and reputation damage. Yet despite a large percentage of cyberattacks targeting Startups, most still lack basic cyber hygiene.


## Are you really a target?

Good question! Most Startups seem to have the mindset that "they're too small to be a target," or "they don't have anything of value." Unfortunately, this mindset is exactly why so many startups get caught out – and then close.

The short answer is, yes. Almost every business has something of value to an attacker. Even your cashflow alone makes you attractive.

You're a target if you manage:

- **Intellectual Property (IP):** Your ideas, designs, code, or processes have value, especially to competitors or anyone looking to replicate your business quickly.
- **Customer data:** Personal, financial, or operational data can be monetised, with value varying by type and volume.

- **Cloud or app hosting (AWS, GCP, Azure, etc.):** Poorly secured accounts can be hijacked and abused to spin up infrastructure for further attacks (proxies, malware delivery, phishing, spam, at your expense.
- **A role in a larger supply chain:** Attackers often target the weakest link to gain access to bigger, better-defended organisations.
- **Healthy cashflow:** Phishing and social-engineering attacks are commonly used to divert payments into attacker-controlled accounts.
- **A heavy reliance on technology for revenue:** Ransomware is a favourite tactic when downtime directly impacts income.

Bottom line: if you run a business, you're a target, regardless of size or industry. From fintech startups to a local coffee shop, no one is too small or too simple to be ignored.

## Planning your cyber budget

One important message is that cyber risk is a business risk, not just an IT problem. While IT provides technical input, strategy and budget decisions should be agreed upon and overseen by the founders. Planning comes down to understanding your risk appetite, current exposures, and where to prioritize resources. Treat this process like any other business risk.

You'll need to understand your cyber risks and exposure to really start to priorities and build out your budget. For early-stage Startups, a practical guideline is to allocate **roughly 5-10% of your tech budget** to cybersecurity, scaling as systems, staff, and digital footprint expand.

Looking at it from a broader business perspective, this often works out to around **1–3% of overall revenue** for startups focused on digital products or customer data. The key is to treat cyber risk as a business risk: invest early in preventative controls and hygiene, and gradually increase spending as exposure grows, ensuring your security posture keeps pace with your growth without overloading your resources.

**Note:** If you're a fintech company, you'll naturally sit at the higher end of the ranges above compared to a business that's less dependent on technology. Ultimately, once you've worked through the process in this handbook, you'll have a clear view of what you need to spend, and why.

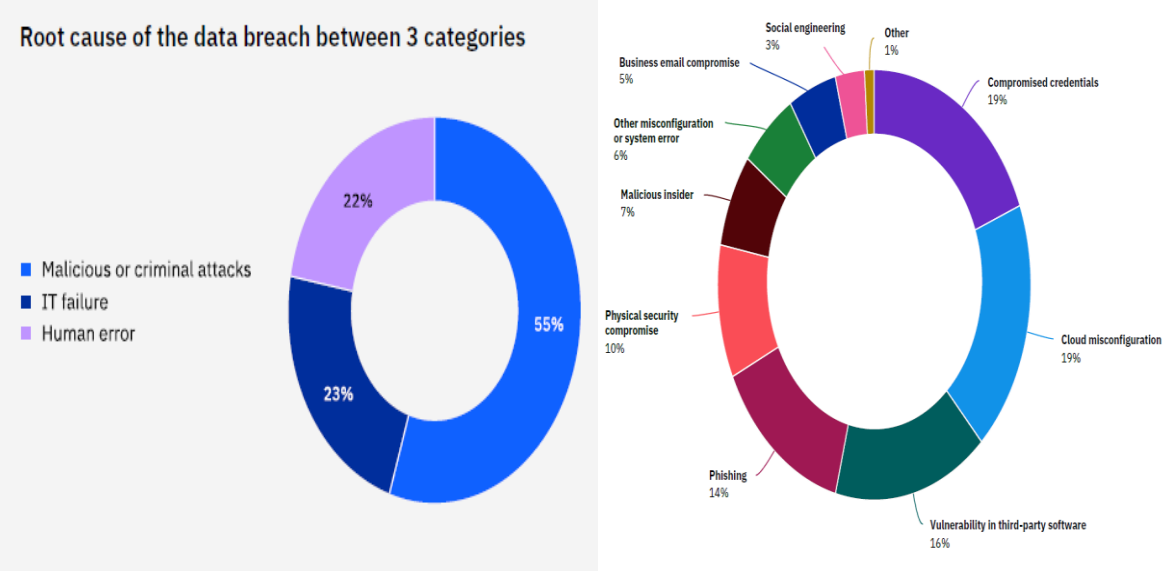
### Prevention is better than cure

This proverb sits at the heart of this handbook. It's the mindset I use to help you protect your startup more effectively, while spending less. Let me walk you through a few key facts, backed by data.

Each year IBM publish a report analysing the sources of cyber incidents [IBM - cost of a data breach]. The findings are clear and haven't significantly changed in the past 5 years. 55% percent of incidents involve malicious attacks - often exploiting poorly maintained or unpatched systems. A further 23% result from IT failures or system errors, while 22% are caused by human error.

Together, these figures highlight a simple truth: most cyber incidents are **preventable** with the right visibility, processes, and leadership attention.

IBM cost of a data breach 2024 and 2020




Summary Don't panic - this is not going to be a technical handbook. You're not expected to have all the answers, and there are tools available to help Startup Founders fill the gaps. That said, understanding your cyber exposure is critical, as it's the root cause of most cyberattacks and the key to protecting your business effectively.

# Chapter 2. Cybersecurity Budget Basics

I'll take you through a set of simple considerations. These will vary depending on the nature of your business, what data you hold, how you operate, and who you work with.

For example, a fintech working with a government agency will be on a very different cybersecurity trajectory and will need deeper, broader controls. But if your business isn't fintech and isn't part of a government supply chain, the following provides a solid starting point.

For startup founders, saying you have no cybersecurity budget is like saying you're going to build a house with no front doors or windows - you're not being bold, you're leaving everything open. The good news is cybersecurity doesn't have to be expensive at the start. Most early protection is simply good hygiene: strong passwords, MFA, patching, backups, access control, and basic monitoring. These small, preventative steps dramatically reduce risk and cost very little.

As your business grows, your data, customers, and exposure grow with it - so should your investment.

## It's not an IT problem

Cybersecurity risks are business risks because they impact where it hurts most: revenue, cashflow, customers, and reputation. A cyber incident can stop sales, delay product launches, trigger regulatory fines, void contracts, and erode customer trust overnight.

While IT teams may manage the systems, the consequences land with founders, executives, and boards who are accountable for financial performance and business continuity. In short, technology is just the delivery mechanism - the real risk is operational, financial, and strategic.

## Just switch stuff on

As mentioned earlier, startups don't need to spend heavily on preventative cybersecurity. With a small team, a few servers, and a limited digital footprint, following the cyber hygiene steps will get you to a reasonably strong cybersecurity profile.

Here are four basic things that are FREE, EFFECTIVE and PREVENTATIVE:

- Free Built-in firewalls and antivirus from Microsoft or Apple operating systems are usually sufficient enough for workstations.
- Free application patch updates- simply ensure auto updates are set on your key applications. You may need to consider servers as a manual update but build that into your maintenance process – it's also free.
- Free Two-factor authentication (2FA): Google or Microsoft authenticator code for servers and for your mobile clients to access servers.
- Security Logs: important for forensics. Ensure you've got this switch on in the servers and workstations – you'll need these later if there's a breach. The difference of a recovery time can be weeks or months without logs.
- Basic preventative cyber hygiene practices are FREE – we cover this in more details later.

Any additional tools should be evaluated based on your risk exposure, potential financial impact, and available solutions in the market. Focus on practical, cost-effective measures first before investing in expensive software.

## Buy Vs Build

When it comes to buying technology versus building it, I lean towards **buy** almost every time. There are plenty of reasons for this, although if your core product *is* the IP you're creating, then clearly, you're in build mode.

So why buy? In my experience, many developers don't design or maintain software with security in mine, including some modern AI development tools. The real risk isn't just the initial build; it's the ongoing maintenance, patching, and security updates. This is where most companies fall short, and where many security breaches originate. I rarely see a realistic budget or long-term maintenance plan baked into internally built solutions.

If a proven product already exists that can be configured to suit your business, I will choose that route. The ongoing cost of security, updates, and resilience is largely transferred to the vendor. Of course, you still need to validate that the vendor has strong security practices and will properly protect your data, but for me, transferring the liability and operational burden of system maintenance is well worth the investment.

## Build with AI

Building technology with AI tools is absolutely fine, but it's important to read the fine print. Be clear on who owns the resulting code and where that intellectual property is stored or processed. Don't assume that security controls are automatically built in or that the code has been properly tested just because it was generated by AI.

AI can accelerate development, but security, ownership, and validation still remain your responsibility.

## Configure, Configure, Configure

Here's the reality: a huge percentage of cyberattacks happen simply because systems are misconfigured. The good news? Fixing configuration issues is usually **free** - and it's one of the most effective **preventative controls** you can put in place. It costs very little to review settings and make the right changes, but the impact on your security posture can be significant.

- Security configuration on email servers to detect fake staff email impersonation from hackers e.g. switch on SPF
- Web security configuration to block cookie stealing e.g. switch on cookie security flags.
- Server configuration to block remote access e.g. switch off SSH port 22

Ok ill stop here as it's getting a bit techy and these are only examples; there are plenty more. The point being, with the right information you can **prevent cyberattacks** with some simple basic free configuration.

## Build a simple risk matrix

Before we move into the next chapter, it's time to start thinking about **risk assessment**. We've covered some cybersecurity basics, but to properly plan a cybersecurity budget, you need a more complete view of your risks.

Keep this process simple. The goal isn't perfection, it's visibility. Start by taking stock of a few core areas of your business and listing them in a simple matrix:

- **Internal solutions:** On-premise or cloud servers, internal applications, and bespoke systems.
- **SaaS vendor applications:** Third-party systems such as Xero for accounting, CRM platforms, HR systems, etc.
- **Data:** The types of data you hold, the volume, and how data moves between systems.
- **Security controls:** The protections in place, such as firewalls, antivirus, MFA, access controls, and monitoring.
- **Policies and procedures:** Any existing security policies, processes, or documented ways of working.

Once this is mapped out, you'll have a far clearer picture of your current risk exposure, and a much stronger foundation for deciding where your cybersecurity budget should be spent.

Summary cyber risk is a business risk, not merely an IT problem. Cybersecurity decisions directly affect revenue, reputation, customer trust, and even the survival of the company. When leadership treats cyber as a technical afterthought, gaps emerge that attackers are quick to exploit.

Founder and executive engagement matters. The most resilient organisations are led by leaders who understand their risk exposure, ask the right questions, and make informed, pragmatic cyber decisions aligned to business priorities. You don't need to be a technical expert - but you do need visibility, ownership, and accountability.

# Chapter 3. Steps for Cyber Budgets

Great! Now that you've mapped out your assets in the simple matrix, it's time to **interrogate what you have**.

I'll guide you through a few key steps, from checking your vendors to assessing your server security. I'll keep this as non-technical as possible, but bear with me, we'll get into the weeds a little later in the chapter.

## Check Your Vendors

Like most startups, you'll rely heavily on AI tools and SaaS platforms to get things done. They're fast, efficient, and save both time and money - what's not to like?

The catch is that you're placing a lot of trust in these providers. They host your data, connect to your systems, and often have deep access to your business. So, this is worth saying loudly: **vendor checks matter**. A little due diligence now can save you a serious headache later.

**Note:** You don't need to go overboard with well-established providers like Microsoft 365, Xero, or Adobe. However, with hundreds of new AI and SaaS apps launching every day, some basic checks are essential, especially for newer or lesser-known vendors.

This isn't an exhaustive list, but these are sensible questions to consider based on the nature of your business. Many answers should be available on the vendor's website. If not, send these as part of an RFI or RFP, reputable vendors will be used to this and should have standard responses ready. If they don't, that's a red flag.

And a final reality check: if you're paying $5 a month for a SaaS tool, don't expect enterprise-grade security. In many cases, security simply hasn't been factored into the price - buyer beware.

**Vendor due-diligence questions to consider:**

- Do you have an established cyber rating? (For example, services like Cygienic can provide independent ratings.)
- Do you hold a current security certification (e.g. SOC 2, ISO 27001)? When was it last audited?
- Has the application been penetration tested? If so, when was the last test?
- Where is customer data stored and where is it backed up? This is critical if data sovereignty applies.

- Do you carry cyber insurance? This helps ensure the vendor can respond financially in the event of a breach.
- Is multi-factor authentication (2FA) enforced for access? This is a baseline requirement today.
- Do you provide named security or customer contact points and a support email?
- What do customer reviews look like?
- Are you listed on any sanctions or watch lists? (You may need to check this independently.)

You don't need perfection - but you do need confidence. If a vendor can't answer basic security questions, it's usually best to walk away.

## Data planning

**Know Your Data: What It Is, Where It Lives, and What It's Worth**

You need to understand what data you hold, where it's stored, and its financial value. This isn't theoretical - it has real cashflow consequences.

For example, if you hold 1,000 EU customer records, store them in Asia, use a third-party provider, and that data is breached - it will cost you and possibly your business.

Here's a simple way to think about it:
The average cost of a breach involving EU personal data is around US$160 per record. That figure includes incident response, user notification, and recovery costs. In this example, **1,000 records = US$160,000** straight off your cashflow. There are nuances in how that cost is calculated, but it's a solid benchmark.

That's before you factor in reputational damage, which for a startup can be existential. On top of that, if the data was not declared or approved for storage outside EU sovereignty, you could face additional regulatory fines, restrictions on operating, or even being struck off business registers.

This is why it pays to know exactly where your data is stored, and what it's worth to the business. If you don't have the balance sheet to absorb that kind of hit, it's time to seriously consider cyber insurance as part of your risk strategy.

**Data Leak:** It's worth checking whether any of your company data is already leaking. There are tools available that can scan the dark web for your information. This step isn't mandatory for every business, but if your company deals with sensitive data, it can be worth taking a look, catching leaks early can save you a lot of trouble down the line.

## When to consider cyber insurance

If your likelihood of a cyberattack exceeds your company's risk tolerance and cashflow, and improving compliance or attack surface scores will take time to resource, it's worth considering a cyber insurance policy. This helps protect your business while you work to strengthen controls and reduce exposure. A good budget tip starts at about **$100 per month** for a basic **$250k** insurance coverage.

## Users are your first line of defense

No cybersecurity handbook would be complete without acknowledging one hard truth: **your staff are often your biggest vulnerability**. As mentioned in Chapter 1, user errors account for **23% of the root causes of cyberattacks**. These errors take many forms: social engineering scams, phishing emails, accidental misconfigurations, and more.

The good news is that **user awareness and training** don't have to be expensive. Even small, consistent efforts make a difference:

- Send regular reminders about phishing emails and what to watch for; there are free resources available to help.
- Teach staff how to manage document shares securely; you'd be surprised how often public shares on platforms like Google Drive are left open.
- Don't forget code repositories; proper access controls here are critical too.

The key point: training your staff doesn't cost much; it just takes time, effort, and focus. Investing a little in awareness now can prevent a lot of headaches later. There, you've **prevented 23% of cyberattacks**, at no or low budget.

## System security configuration prevention

According to the IBM *Cost of a Data Breach Report*, around **55% of breaches stem from malicious attacks**, and a large portion of exploits are misconfigured or poorly maintained internet-facing servers. If your organization has such servers, they should be a priority for review.

Focus on these before your internal (on-premises) servers, especially if your "crown jewels" are exposed to the internet. While hiring a professional penetration testing team is ideal, it can be costly. If your budget is tight, you can still "kick the tyres" using

vulnerability scanners or Attack Surface Management (ASM) tools - many of which are free or inexpensive to budget - refer to Chapter 6 for more details.

ASM scanners are like a pentest lite assessment: they won't dive as deep as a full penetration test, but they give a strong overview of your internet-exposed assets. They can help you identify low-hanging security risks quickly. Beyond scanning servers, many tools also check email systems, potential compromises, and external indicators of risk, giving a broader view of your attack surface.

The key is to keep it simple and actionable, address the easy wins first while keeping an eye on the bigger picture.

## Shared office Vs fixed office

If you work in a shared office space like WeWork, you're relying on their security infrastructure e.g. firewalls, routers, and Wi-Fi. A good tip: **ask for a security certificate** for their infrastructure, ideally signed off by a qualified architect. This gives you confidence in the baseline protections in place. Now you can request your own infrastructure but that will put more cost on to your company.

If your email and data sharing are properly encrypted, you'll likely be fine for most tasks. But if you handle **sensitive client data**, shared spaces can become limiting, and having your own controlled environment may be the safer choice.

If you have the luxury of your own office, you can choose to host your own infrastructure, though this usually comes with extra costs for hardware and dedicated ISP lines.

I would recommend a share office to keep costs down initially, but your working practices need to be super security conscious, don't leave confidential papers lying around, don't talk shop in public areas, and make sure your data is encrypted when using Wi-Fi and the internet.

Summary The key point here is that effective cybersecurity budgeting starts with understanding your risks. When you know where your real exposures are, you can make smarter, well-informed decisions instead of spending blindly.

For example, if you identify that your systems don't use multi-factor authentication, you can plan a small amount of development or configuration time to address it. The cost is minimal, yet it removes a significant risk from your business. This is how good cyber decisions work, low effort, high impact, driven by visibility rather than fear.

# Chapter 4. Scaling Securely Without Slowing Down

As your startup grows, cybersecurity should grow with the company, not be treated as a one-off task. For early-stage SMEs, a practical guideline is to allocate roughly 8–15% of your IT budget to cybersecurity, scaling as systems, staff, and digital footprint expand.

Looking at it from a broader business perspective, this often works out to around 1–3% of overall revenue for startups focused on digital products or customer data. The key is to treat cyber risk as a business risk: invest early in preventative controls and hygiene, and gradually increase spending as exposure grows, ensuring your security posture keeps pace with your growth without overloading your resources.

## Legacy System Trap

Founders should be especially wary of legacy systems, outdated software, servers, or tools that were never fully updated or patched. While they may "just work" today, these systems often contain vulnerabilities that attackers know how to exploit, and over time they become a hidden liability. Staying current with updates, patches, and modern platforms isn't just a technical task - it's a business decision.

Regularly refreshing systems reduce the risk of breaches, lower long-term maintenance costs, and ensure your company isn't exposed to risks that could derail operations, harm your reputation, or create expensive recovery scenarios down the line.

## Continuously Monitor Risk

For startup founders, managing cyber risk manually can quickly become a heavy overhead as your team and digital footprint grow. Wherever possible, continuous monitoring of cyber risks should be automated - tracking vulnerabilities, system changes, third-party exposures, and compliance gaps in real time. Automation reduces the day-to-day burden on you and your team, ensures nothing slips through the cracks, and provides instant visibility when risks arise. By building automated monitoring into your cybersecurity strategy, you can stay ahead of threats while keeping your focus on scaling the business.

## Cyber Assurance as a Growth Enabler

Startup founders should be aware that upstream partners, investors, and customers increasingly request ongoing cyber assurance as part of due diligence and operational

confidence. Managing these requests manually can be time-consuming and inconsistent.

That's why it's essential to be on top of this, highlighting how you track, manage, and report on your cybersecurity posture. Continuous assessments, compliance checks, and risk reports should be automated and made available on demand, giving stakeholders confidence while freeing your team from repetitive reporting tasks.

## What investors like

For investors, you're thinking ahead and you're showing maturity to grow into a Unicorn. You would be surprised how many do nothing and then wonder why it all went wrong! Overall, it lowers downside risk and increases confidence in execution; for partners, it builds trust and speeds up due diligence; and for customers, it reassures them their data and operations are in safe hands. Done well, cybersecurity stops being a cost or a blocker and becomes proof that your business is credible, resilient, and ready for long-term success.

## What good cyber looks like

Good cybersecurity isn't about having the flashiest tools - it's about measurable, manageable practices that protect your business and build confidence with stakeholders.

For startups, this means aiming for an Attack Surface (ASM) rating of a B, a compliance level of B, is good enough. Just ensure you have assessed the risks we discussed in the other chapters, and you have a commonsense plan.

When these elements are in place, you're not only protecting your data and systems - but you're also building a resilient, scalable foundation that investors, partners, and customers can trust.

Nothing is ever 100% secure. But when you take reasonable, visible steps to protect your business, customers, investors, and partners gain confidence in your approach. That trust earns you the benefit of the doubt when issues arise - and turns cybersecurity into a business enabler rather than a blocker.

## Competitive Edge

Good cybersecurity practices, combined with regular monitoring and reporting, are no longer just operational necessities - they're a competitive advantage. In today's market,

clients and partners expect proof that their data is safe, and the ability to demonstrate ongoing cyber assurance can be the difference between winning or losing a pitch. Startups that can show clear risk management, up-to-date compliance, and continuous monitoring stand out as trustworthy, professional, and prepared for growth, giving them a measurable edge over competitors who cannot provide the same assurance.

## When to hire a cyber expert

As your business grows, you might think about hiring someone to manage compliance and cybersecurity. However, a well-designed system should minimize the need for specialized technical experts, allowing you to manage cyber risk with a junior tech hire or even a non-technical manager from another discipline. Consider fractional CISOs as an option to just pop in a few times a month to assess things and make sure it's all going according to plan.

Tools like CyberIQ shift the role from a technical specialist to more of an administrator of cyber risk, streamlining processes, automating monitoring, and reducing hiring costs while keeping your cybersecurity program effective.

Summary As your company grows, so do the demands place on it - by supply chains, investors, regulators, auditors, customers, and other stakeholders. Over time, these expectations compound and you reach another crossroads: where should you invest next in cybersecurity?

Typically, this stage brings new challenges. More staff and more systems increase identity and access management complexity. Larger customer databases introduce stricter regulatory and compliance requirements. At the same time, your digital footprint expands and with it, your risk exposure. Growth and cyber risk are tightly correlated.

The good news is you won't be starting from scratch. By this point, you'll already have visibility into your risks and a clear plan in place. That roadmap allows you to invest gradually and intelligently, aligning cyber spend with real, emerging risks rather than reacting under pressure or overspending out of fear.

# Chapter 5. The Top 5 cyberattacks targeting Startups

We're going to dip slightly into the weeds here; it gets a bit technical in this chapter - but I'll keep it light and practical and will help you think about where to invest.

There are hundreds of cyber-attack vectors, but in reality, most attacks focus on what we'd call "wholesale targets." These are mass-market attacks that work on a volume game: attackers cast a wide net knowing that even a small success rate delivers results.

Because so many organizations share the same weaknesses, a surprising number still fall for the same common attacks – ill cover how and why in this section.

## 1. Email phishing

No.1 cyberattack vector is email-phishing: 70-90% of cyberattacks start from phishing email or social engineering, the main reason is because it's cheap and easy.

This is the most common way startups get breached. Someone clicks a realistic-looking email or login page and unknowingly gives away their password. From there, attackers can access email, systems, and business tools, hold you to ransom, or deny you access.

**Why Startups are at risk:** People are busy, security training is light, and accounts are often shared to save money.

## 2. Confidential data leaks

Publicly shared documents that are left open and unchecked, containing business account details, contact information, or system configurations - are a common goldmine for attackers. This information is frequently discovered, collected, and shared between hacker groups. Data exposed through Google Drive links, insecure FTP sites, Microsoft document shares, developer repositories, and similar platforms all feeds attacker reconnaissance, helping them plan and weaponize an attack.

**Why this happens in Startups:** Startups move fast. Documents are created quickly, reused from old templates, shared for convenience, and rarely reviewed again. Access settings are configured once, then forgotten, quietly leaving sensitive information exposed.

## 3. Weak password, stolen credentials and SaaS tooling

Weak passwords and systems without multi-factor authentication (2FA) are linked to an estimated 60–80% of cyberattacks. In most cases, attackers aren't breaking in directly - they're using stolen credentials. Email addresses and login details are commonly harvested from breaches of other platforms, then shared or sold within criminal groups.

This is why your own systems are often not the weakest link. The real risk comes from third-party tools and services with poor security controls. Founders and employees frequently reuse their company email and password when signing up for external SaaS products. Once those credentials are exposed, any internal system or other Saas subscription without 2FA becomes an easy target.

**Startups naturally gravitate toward affordable tools**: Unfortunately, price often reflects the level of security investment behind a product. Ultra-low-cost SaaS tools - sometimes just a few dollars a month, may not have built in adequate security controls, making them attractive targets for attackers and a hidden risk to your business.

## 4. Website and application security flaws and maintenance

System updates and configuration issues are responsible for an estimated 30–40% of cyberattacks. Poorly configured or unpatched systems create easy entry points for attackers. Even small configuration mistakes, or delayed security updates in websites and applications can allow attackers to bypass controls or extract large volumes of sensitive data.

**Common Startup mistake:** You've built or adopted a great application to support the business - but security wasn't a core design consideration. That's understandable. The pressure is to ship fast, control costs, and get to market. Security often becomes an afterthought because it slows things down and consumes budget.

## 5. The 3rd party supply chain risk

The third-party supply chain is the root cause of roughly 30% of cyberattacks. Startups are frequently targeted not because of who they are, but because of who they connect to. Access to a startup's systems can provide attackers with a stepping stone into larger customers, partners, or ecosystems.

**Startups often become the downstream compliance and security headache**: Attackers rarely go after the most secure organisation first - they look for the weakest

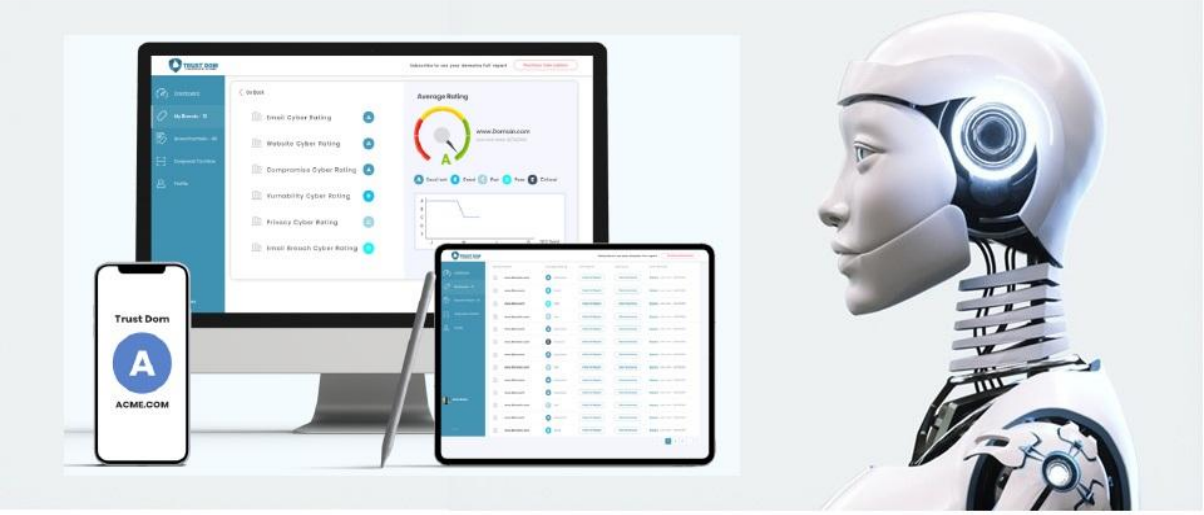
link in the chain. Smaller companies typically have fewer controls, less monitoring, and limited security budgets, making them an attractive and efficient entry point.

For founders, this means cyber risk doesn't stop at your own environment. Your security posture directly impacts your customers and partners, and increasingly determines whether you can win deals, pass due diligence, or even stay in a supply chain at all. Managing third-party risk is no longer optional - it's a business requirement.

Summary These risks are common, well understood, and largely preventable with some basic, targeted preventative controls. In many cases, organizations aren't breached because attackers are sophisticated, they're breached because simple checks were never done.

In the next chapter, I'll show how these risks can be quickly identified and reduced using a lightweight, practical tool called CyberIQ. It's not about boiling the ocean or turning you into a security expert, just giving you clear visibility into your exposure and helping you fix the most likely problems first.

Cygienic CyberIQ 2026



# Chapter 6. Preventative Cybersecurity with CyberIQ

If a large share of cyber incidents come from the same top five attack paths, then prevention is really about addressing those risks early, before they turn into real problems.

The good news is this doesn't require heavy spending or complex security programs. Most of these risks can be significantly reduced with simple, preventative measures and a small number of well-chosen tools. In other words, getting the basics right goes a long way.

CyberIQ is designed to bring cyber risk intelligence to you, so you can make better-informed, business-led decisions, not technical guesses. Beyond identifying risks, CyberIQ helps quantify them by calculating:

- **Financial exposure**
- **Data valuation**
- **Estimated data breach costs**
- **Likelihood of a cyber incident**
- **Indicative cyber insurance costs**

This turns cybersecurity from a vague technical concern into something you can measure, prioritise, and manage like any other business risk.

## Email phishing prevention

We can address this challenge in several ways using CyberIQ modules - specifically the Cyber Library and ASM. This module helps identify risks, track vulnerabilities, and provide actionable guidance so you can proactively strengthen your security posture.

- **CyberIQ User Awareness:** Provide staff with a simple, easy-to-follow guide that helps them recognise suspicious emails before they click. CyberIQ includes email phishing awareness material that you can quickly adapt and reuse. Simply distribute it to staff in PDF format, giving them clear examples of what to look out for and reinforcing safe behaviour without adding training overhead.

- **Social Engineer:** Add new processes to double check things before a new request is made to transfer money, change data, share any credentials, or give access to someone – the old CEO scam email requesting urgent money transfer simply needs

a call back and a share the secret code process. If a company has changed its bank details via email, again a call them and check before making the change.

- **CyberIQ Email:** the ASM module to scan your email systems and check whether phishing emails from outside your company can be detected and blocked. Start with basic configurations like SPF, DKIM, and DMARC settings - your email provider can help ensure these are correctly set up. Regularly verifying these settings strengthens your defences against common email-based attacks.

## Data leak prevention

**CyberIQ Data Leak:** this module lets you search for potential leaks by targeting specific keywords or domains. For example, user credentials often appear on hacker paste sites or in other dark web locations. Simply enter your company domain, and the system scans for exposed assets. You can also extend the search to areas like developer code repositories, where system configurations or access credentials may have been accidentally left behind.

## Weak password, stolen credentials prevention

**CyberIQ Email Breach:** This feature scans your domain against online cyber services that track compromised email accounts. If any company emails are flagged as compromised, the system immediately notifies you – the request would be to notify staff so they can reset their passwords and prevent unauthorized access. Regular use of this tool helps reduce the risk of account takeover and keeps your business protected.

## Website and application security flaws prevention

**CyberIQ Attack Surface:** Your attack surface is the most common entry point for attackers and should be a primary focus for identifying misconfigured or unpatched internet-facing systems. While internal (non-internet-facing) servers should also be assessed, external systems carry the highest risk, and weaknesses exposed externally often indicate similar gaps internally.

## 3rd party supply chain risk prevention

**CyberIQ 3rd Party Portfolio:** The portfolio module allows you to assess your third-party ecosystem using a two-pronged approach. First, run non-intrusive, passive attack-

surface scans on suppliers and partners to identify externally visible weaknesses, without touching their systems. Use the same online service provider you use to measure your own attack surface.

Second, issue a simple cyber compliance questionnaire (with optional financial surveys) to assess the maturity and credibility of their responses. You can send a spreadsheet, google form or use a paid service to centrally manage and rate each response.

## Automate Reports

Startup founders should be prepared to regularly present cybersecurity updates to boards, investors, and auditors. Even if your team is small, stakeholders will expect clear, accurate, and up-to-date reports on your cyber risk posture, compliance, and mitigation efforts. Using CyberIQ can help automate much of this process, providing dashboards, risk scores, and ready-to-share reports so you can deliver consistent, professional updates without it becoming a full-time burden.

This allows you to focus on growing the business while maintaining confidence that your cybersecurity reporting is reliable and audit ready.

CyberIQ™ Using a single platform to manage these preventative steps is the most effective way to reduce cyber risk. CyberIQ does exactly that, clearly highlighting where risks exist throughout your business and giving you a practical, structured way to manage and reduce them over time. It's not just about identifying issues; it's about maintaining visibility and control, so risks are addressed before they become incidents.

CyberIQ dashboard 2026