IT GOVERNANCE USA | GREEN PAPER

Cybersecurity 101

A guide for SMBs

Protect • Comply • Thrive

Introduction

Every day, thousands of businesses around the world are attacked by cyber criminals. The costs can run into many millions of dollars – a 2020 IBM report puts the average cost for US businesses at $8.64 million per breach.[1]

Fortunately, this amount decreases substantially for small and medium-sized businesses (SMBs). Nonetheless, with both direct costs (like a server going down, or data loss necessitating rework) and indirect costs (such as loss of consumer confidence, or service unavailability resulting in lost business) to consider, a single attack can easily amount to thousands of dollars.

More to the point, SMBs are frequently attacked. Although most SMBs are aware of the general threats within the cyber landscape, 66% believe it unlikely they will be attacked – a clear misconception, since 67% experienced an attack over a 12-month period.[2]

This is not the only misconception when it comes to cybersecurity. For instance, it is commonly – and wrongly – believed that only computers and external threats need to be considered. However, there are also misunderstandings that, once cleared up, will actually work in your favor. Contrary to popular belief, cybersecurity is not about technology alone and does not need to be expensive. As long as you take a strategic approach, you will find cybersecurity accessible, affordable, and manageable.

Six cybersecurity myths

Before delving into strategy, it is worth debunking some myths to help you avoid common mistakes.

Myth 1: My organization does not have anything worth stealing

On the contrary – practically every organization, including small ones, holds valuable information, such as payment details, customer and employee personal data, or intellectual property. The 2020 Verizon Data Breach Investigations Report found that small businesses suffered 28% of all breaches.[3] Many attacks are opportunistic, targeting vulnerabilities rather than organizations, so SMEs are just as much a target as anyone. It is often not about how valuable your data is, but how easy it is to compromise it.

Take the case of a UK real estate agency. Due to a misconfiguration that was not fixed for nearly two years, there were no access restrictions to a server that contained the data of 18,610 individuals.[4] During those two years, there were 511,912 anonymous logins from 1,213 unique IP addresses. Shortly after, a criminal hacker demanded a ransom in return for not releasing information about its customers. The agency may be small, but that did not make it safe.

Not just confidentiality

It is worth noting that cybersecurity is not solely about safeguarding data from theft, or protecting its confidentiality (making information only accessible to authorized users). There are two further important aspects of cybersecurity management: integrity (ensuring the information is complete and accurate) and availability (authorized users can access it as and when necessary). Imagine not being able to access your IT systems for a day, a week, or longer – the consequences could easily snowball.

Myth 2: Security is not affordable

Before you allow yourself to be put off by the cost of any security measures, remember that allowing your organization to be cyber insecure can prove an expensive mistake. A 2020 Hiscox report found that the mean cost of an incident for micro, small, and medium-sized businesses respectively is $4,359, $9,225, and $58,750.[5]

Second, consumers are concerned about having their technology compromised – according to a KPMG report, 78% are concerned for apps, 74% for Wi-Fi, 69% for the Internet of Things (IoT), and 67% for the Cloud.[6] According to the same report, a sensitively handled cyber incident – and incidents are an inevitable occurrence according to half of the responding CEOs – would actually reinforce consumer trust, making security not just an expense or a way of avoiding revenue loss, but actually a means of generating revenue, particularly in the long term.

Showing that you take cybersecurity and data privacy seriously will reassure customers, partners, and employees, as well as help you appeal to new clients. Achieving certification to a recognized scheme like ISO 27001 (the international standard for information security management) is one way of proving your commitment to security, but you could also do things like publish a cybersecurity policy.

Myth 3: Cybersecurity is about technology alone

While technology created the need for cybersecurity, it is not a matter that can be managed by technology alone. People are your first line of defense; they are the ones who need to avoid malicious links and files, and they play critical roles in preventing more pedestrian breaches, like losing a USB stick or allowing an intruder into the building.

Unfortunately, people also tend to be the weakest link in the security chain. For instance, a 2020 Trustwave report found that 50% of incidents originated from phishing or other forms of social engineering – in other words, half of all cyber incidents were caused by users being tricked into clicking a malicious link or downloading a malicious attachment.[7] And that is just one way human error can lead to a security breach.

At the end of the day, humans are fallible. And they are especially fallible when they are busy, multitasking, or distracted. Just one careless employee can cost your organization thousands of dollars, if not more.

Myth 4: Cybersecurity is for IT to manage

While IT plays an important role in an organization's cybersecurity, it is just one part of the picture. A 2019 Keeper Security report makes clear that there is a lot of confusion about who is actually responsible, with respondents giving wildly different answers.[8] In fact, *everyone* in an organization is responsible for keeping the business secure. As we saw in myth 3, any member of staff can present a risk.

Furthermore, the board's role is often underestimated: If the top of the organization takes an active and visible interest in security, it is much more likely the rest of the business will follow suit. Moreover, considering how interconnected technology and business are, not to mention how severe the impact and cost of a cyber incident can be, cybersecurity should be a high priority on the board's agenda.

Myth 5: Cyber threats are external only

Although many threats are indeed external, plenty originate from within your organization, whether intentional or not – 60% of organizations responding to a 2019 Haystax report confirmed that they suffered an insider attack in the past 12 months.[9]

Typical 'enablers' to the accidental internal threat include weak/reused passwords, unlocked devices, bad password-sharing practices, and unsecured Wi-Fi networks – reiterating the point made in myth 3: People are fallible, especially when it comes to security. However, the insider threat can also be deliberate (originating from disgruntled or blackmailed employees, for instance), with enablers like over-privileged users, and the volume of data collected and stored.

Myth 6: Only PCs and laptops can be affected by viruses and malware

In fact, mobile malware is extremely widespread, and any smart device can be hacked. That includes smartphones, tablets, and any other device connected to the Internet. These newer technologies tend to offer limited security, as mobile antivirus software is not as widespread as it should be. Furthermore, company devices can be very attractive targets, as they store and/or have access to a lot of confidential information.

Mobile devices are not just vulnerable through malicious apps. Jailbreaking or rooting, which allows you to get around manufacturer safeguards, can also seriously impact your device's security. Furthermore, the size and portability of such devices puts them at greater risk of loss and theft.

Thinking about strategy

Based on these myths, there are six important points to remember:

1. Any organization is a target
2. Taking a strategic, risk-based approach can make security significantly more affordable
3. Humans are fallible
4. Security is a matter for everyone – including the board
5. External threats are real – but so is the internal threat
6. Mobile devices are significant vulnerabilities, too – not just your computers

These points can form the basis of an initial strategy that takes a balanced approach, broadly covering the key elements of cybersecurity, while addressing the more significant risks first. They are also a suitable starting point as they can be tackled fairly easily and affordably.

As you gain a clearer picture of the risks you are addressing and become more confident in your approach, you can develop that base into a more comprehensive and structured strategy that looks to gradually improve and mature your cyber defenses.

Basic measures you should take

This section discusses in more concrete terms the measures you need to consider – not just because they are effective and affordable, but because they do not require you to be a cybersecurity expert.

Risk assessments

The first step to cost-effective defense is finding out exactly what threats and vulnerabilities can harm your business the most, and making sure those risks are addressed. In other words, before you think about what measures to implement and how much to spend on them, you need to conduct a risk assessment – it will help you understand exactly what risks your organization faces and how to prioritize addressing them.

Staff training and awareness

To reiterate one of the most important lessons in cybersecurity: Humans are your weakest link, especially when they are busy, multitasking, or untrained. Staff training keeps employees vigilant and can teach them, among other things:

- How to recognize phishing scams
- What to do if they become aware of an incident or breach
- The dos and don'ts of passwords
- To be careful about what they write on social media
- What to pay attention to when working remotely

The goal is to help avoid the most common, preventable breaches caused by human error, which can be achieved in different ways. You could use a bespoke training solution that accounts for the most likely scenarios your employees may face, but there are also quicker and cheaper options available, such as off-the-shelf e-learning.

Policies and procedures

Documented policies and procedures are invaluable to help guide employees in specific situations, such as reporting a potential breach. They also clearly demonstrate your organization's – and the board's – standpoints on security, which can in turn help build a security culture throughout your organization.

A good and properly enforced policy can prove a more effective way of changing staff behavior than sophisticated (and expensive) technological measures. There are a few golden rules to follow that can help you create effective policies and procedures:

- Keep them realistic. A policy or procedure needs to instruct, but it also needs to be practicable – if it is overly idealized, it is unlikely to be effective.
- Talk to the people who will be required to follow those procedures and incorporate their input.
- Check for possible process inefficiencies (because two different policies cover the same point, for example), and eliminate them.
- Keep your procedures as clear and straightforward as possible. If they are too complicated or hard to understand, staff are unlikely to follow them.
- Procedures are extremely likely to change with time, so should be regularly reviewed and, where necessary, updated.

If you find it tricky to decide what policies you need or what to cover in them, you may find it beneficial to use customizable templates as your starting point.

Passwords

No matter your organization's exact requirements, we recommend implementing a strong password policy, given that people generally have terrible password habits. Worldwide, 24.2 million breached accounts had '123456' as their password.[10] And those who do set better passwords are prone to writing them down or using them across accounts. In one notable example, TV5Monde, a French television network that broadcasts internationally, filmed a piece on its premises while social media passwords were visible in the background.[11]

Basic technological measures

Although the most suitable technological controls will vary per organization, the following five provide a good starting point:

1. **Firewalls**
   Use and configure firewalls (which work as a barrier) to secure your Internet connection, particularly when using public or other untrusted Wi-Fi networks.

2. **Secure configuration**
   The default configurations on devices and software are often as open as possible, allowing for maximum convenience, but also providing more access points for unauthorized users. Improve your security by, for example, disabling or removing any unnecessary functions and changing default passwords to reduce the risk of a security breach.

3. **Access control**
   Earlier, we saw that the internal threat can be a serious one, intentional or not. Giving a lot of people access to your data and services also means that there are more accounts that, if compromised, can lead to a more serious breach of security. Ensuring that access is given on a 'need-to-know' basis only, with 'access denied' as the default option, will help reduce the scope for a breach.

4. **Protect from viruses and other malware**
   Malware such as viruses can infect your systems when, for example, an employee falls for a phishing scam, but they are also commonly introduced through removable storage drives like USB sticks. You can protect yourself from malware by using anti-malware software, and 'whitelisting' and 'sandboxing' techniques.

   ('Whitelisting' involves creating a list of applications permitted on a device, and blocking any application not appearing on that list from running. 'Sandboxing' involves running an application in an as isolated an environment as possible, giving it limited access to the rest of your networks and devices.)

5. **Keep devices and software up to date**
   Manufacturers and developers normally release regular updates that not only improve the software but also fix or 'patch' any discovered vulnerabilities. Installing those updates as soon as they are available minimizes the time frame in which those vulnerabilities can be exploited. If the manufacturer stops offering support for the hardware/software you are using, it is time to replace it with a more up-to-date alternative.

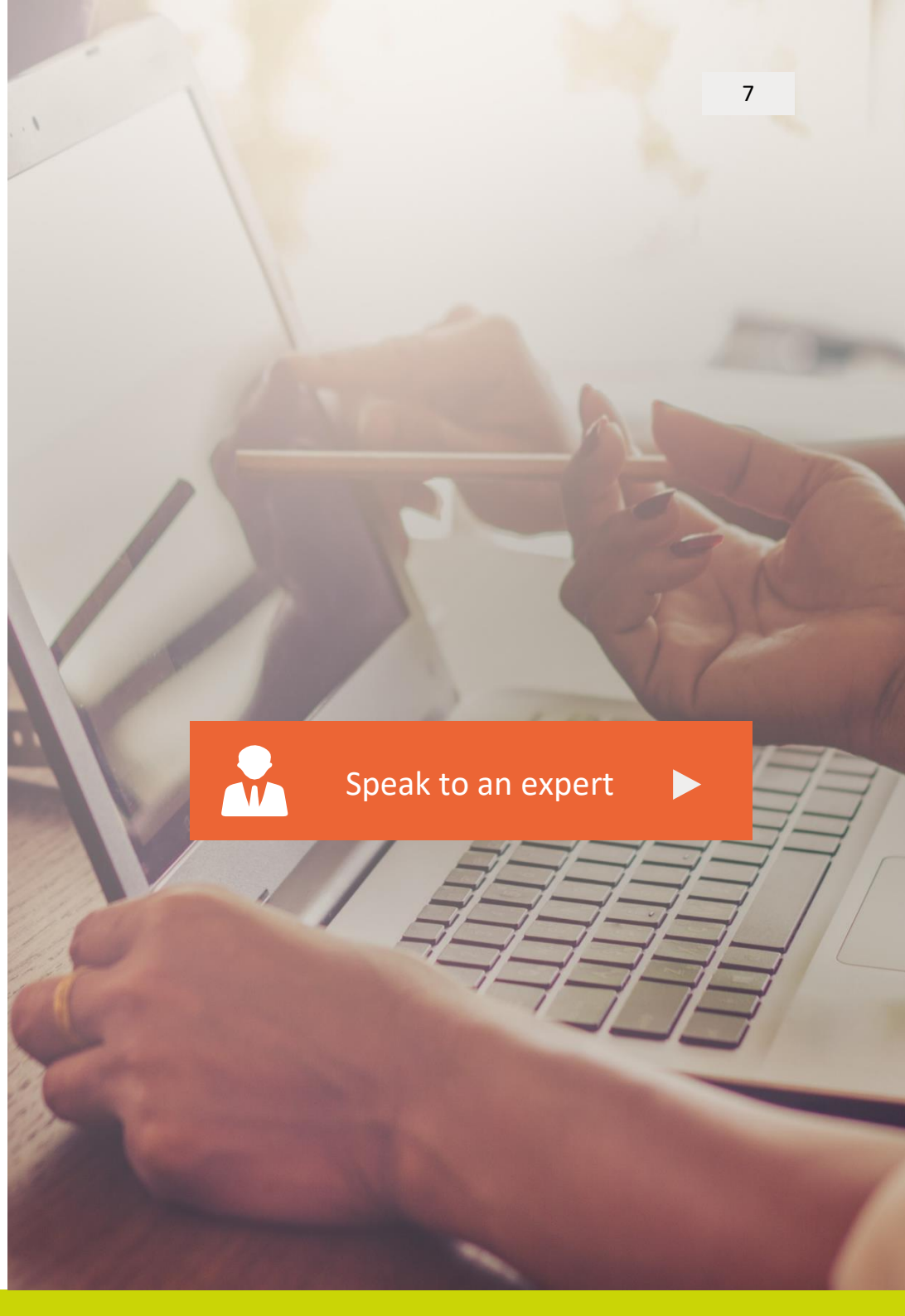
Conclusion

Taking a strategic approach to cyber threats is critical as technology becomes more pervasive, and criminals become more adept. A strategic, risk-based approach also helps ensure the most serious risks are addressed, while keeping the mitigating measures as cost-effective as possible. It also allows obstacles – such as misunderstanding the true nature of the cyber landscape, a lack of resources, or a lack of management support – to be identified and overcome at an early stage.

Taking this approach identifies the critical objectives for an effective cybersecurity strategy:

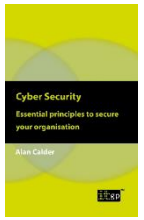
- Risks to the organization's information and information systems are assessed using a consistent and reliable process.
- Staff are trained to use technology securely.
- Staff understand the risks, and what they can do to mitigate them.
- Policies and procedures that support cybersecurity have been developed and are regularly reviewed. These should also demonstrate clear board commitment to cybersecurity.
- Technological measures to protect the organization's information and information systems (such as the ones discussed earlier) have been implemented and are regularly assessed to ensure they are working correctly.

Establishing such objectives and putting measures in place to achieve them is a good starting point for your organization's cybersecurity strategy. Just remember to treat cybersecurity issues as any other business risk; being small does not make you safe. If anything, it makes you more vulnerable – and just one weakness exploited can wreak havoc. Cybersecurity may cost, but cyber insecurity can cripple.



Useful cybersecurity resources

IT Governance USA offers a unique range of cybersecurity products and services, including books, software, training courses, and professional consultancy services.



Cyber Security: Essential principles to secure your organisation

This handy pocket guide takes you through the fundamentals of cybersecurity, the principles that underpin it, vulnerabilities and threats, and how to defend against attacks.

Information Security Staff Awareness E-Learning Course

Mitigate the risk of a security breach or incident by boosting employee awareness of information security threats with this staff training course.

CyberComply

This Cloud-based solution makes compliance with cybersecurity and data privacy requirements simple and affordable. With wizards, databases, and prompts guiding you all the way, you can get started without any expert knowledge.

Certified Cybersecurity Foundation Self-Paced Online Training Course

Get a comprehensive introduction to the key aspects of cybersecurity. Gain knowledge of cybersecurity, the threat landscape, threat intelligence, incident response, and more.

Vulnerability Scan

This fast, fully automated external vulnerability scan of your Internet-facing IT assets enables you to quickly identify vulnerabilities and misconfigurations in your websites, applications, and infrastructure.

Cybersecurity for IT Support Self-Paced Online Training Course

Train your IT support department on the most common cyber attacks and build awareness around the importance of effective cybersecurity with this online course.

Cyber Health Check

Easily identify your cyber risks, assess your risk exposure, and identify a practical route to minimizing those risks with this four-phase consultancy service.

Simulated Phishing Attack

A simulated phishing attack will establish whether your employees are vulnerable to phishing emails, enabling you to take immediate remedial action to improve your cybersecurity posture.

Other papers you may be interested in

Cybersecurity and ISO 27001
Reducing your cyber risk

EU General Data Protection Regulation
A compliance guide

IT Governance USA solutions

IT Governance USA is your one-stop shop for cybersecurity and IT governance, risk management, and compliance (GRC) information, books, tools, training, and consultancy.

Our products and services are designed to work harmoniously together so you can benefit from them individually or use different elements to build something bigger and better.

Books

We sell sought-after publications covering all areas of corporate and IT governance. Our publishing team also manages a growing collection of titles that provide practical advice for staff taking part in IT governance projects, suitable for all levels of knowledge, responsibility, and experience.

Visit www.itgovernanceusa.com/shop/category/it-governance-usa-books to view our full catalog.

Toolkits

Our unique documentation toolkits are designed to help organizations adapt quickly and adopt best practice using customizable template policies, procedures, forms, and records.

Visit www.itgovernanceusa.com/documentation-toolkits to view and trial our toolkits.

Training

We offer training courses from staff awareness and foundation courses, through to advanced programs for IT practitioners and certified lead implementers and auditors.

Our training team organizes and runs in-house and public training courses all year round, as well as Live Online and self-paced online training courses, covering a growing number of IT GRC topics.

Visit www.itgovernanceusa.com/training for more information.

Consultancy

We are an acknowledged world leader in our field. Our experienced consultants, with multi-sector and multi-standard knowledge and experience, can help you accelerate your IT GRC projects.

Visit www.itgovernanceusa.com/consulting for more information.

Software

Our industry-leading software tools, developed with your needs and requirements in mind, make information security risk management straightforward and affordable for all, enabling organizations worldwide to be ISO 27001-compliant.

Visit www.itgovernanceusa.com/shop/category/software for more information.

IT Governance USA is the one-stop shop for cybersecurity, cyber risk, and privacy management solutions. Contact us if you require consultancy, books, toolkits, training, or software.

t: +1 877 317 3454
e: servicecenter@itgovernanceusa.com
w: www.itgovernanceusa.com

A GRC International Group plc subsidiary

420 Lexington Avenue, Suite 300
New York, NY 10170, USA

IT Governance USA Inc.

@ITG_USA

/it-governance-usa-inc

@ITGovernanceUSA

Endnotes

[1] IBM, “Cost of a Data Breach Report 2020”, July 2020, https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/.

[2] Keeper Security, “Cyber Mindset Exposed: Keeper Unveils its 2019 SMB Cyberthreat Study”, July 2019, https://www.keepersecurity.com/blog/2019/07/24/cyber-mindset-exposed-keeper-unveils-its-2019-smb-cyberthreat-study/.

[3] Verizon, “2020 Data Breach Investigations Report”, May 2020, https://enterprise.verizon.com/resources/reports/dbir/.

[4] Information Commissioner’s Office (the UK data protection regulator), “Monetary Penalty Notice – Life at Parliament View Limited”, July 2019, https://ico.org.uk/action-weve-taken/enforcement/life-at-parliament-view-limited/.

[5] Hiscox, “The Hiscox Cyber Readiness Report 2020”, July 2020, https://www.hiscox.co.uk/cyberreadiness.

[6] KPMG, “Consumer Loss Barometer 2019 – The economics of trust”, April 2019, https://home.kpmg/xx/en/home/insights/2019/04/trust-in-the-time-of-disruption.html.

[7] Trustwave, “2020 Trustwave Global Security Report”, April 2020, https://www.trustwave.com/en-us/resources/library/documents/2020-trustwave-global-security-report/.

[8] “Cyber Mindset Exposed: Keeper Unveils its 2019 SMB Cyberthreat Study”.

[9] Haystax, “Insider Threat Report – 2019”, August 2019, https://haystax.com/wp-content/uploads/2019/07/Haystax-Insider-Threat-Report-2019.pdf.

[10] Troy Hunt, “Pwned Passwords”, *Have I Been Pwned*, accessed February 2021, https://haveibeenpwned.com/Passwords.

[11] Loek Essers, “Hacked French broadcaster’s passwords revealed in TV broadcast”, *IDG News Service*, April 2015, https://www.csoonline.com/article/2908852/hacked-french-broadcasters-passwords-revealed-in-tv-broadcast.html.