STRIPE OLT

CYBER SECURITY

How will you manage yours?

INTRODUCTION

According to the World Economic Forum's 'Regional Risks to Doing Business Report' [1], cyberattacks "not only remained the number-one risk for businesses in the US, Canada, the UK and Germany, but also edged out all other risks in France and Italy to occupy the top spot for the first time." Across the world, cyberattacks were seen by CEOs as the second biggest risk of doing business overall, only beaten by fiscal crises as potential disruptors.

Martin [2], Operations Director at a risk management consultancy, tells us: "We are acutely aware of the risks not just for loss of data, but also for our reputation and clients' reputations."

Daniel, partner at a leading law firm, agrees: "Even if your systems mean that you do not lose any data, an incident can result in a core loss of trust with your clients and suppliers."

SIZE ISN'T EVERYTHING

Traditional approaches to cyber security have often been based on the assumption that the bigger the organisation, the more security it needs – and can afford. This results in cyber security strategies that scale with the organisation: small start-ups or fledgling businesses can fall into the trap of not thinking too hard about the security of their infrastructure, but as the organisations mature, so does their approach.

As a recent McKinsey report points out [3], however, this way of thinking has had its day. Changes in the structure of work, the growth of a mobile and freelance workforce, data security regulations and the developing eco-systems of start-ups working on sizeable projects or with large organisations mean that it's no longer safe to assume that small organisations are doing small, low-risk things. These changes, coupled with the explosion of businesses dealing with huge amounts of data, even as relatively small operators, mean that the 'size=risk=security budget' way of thinking is no longer relevant.

London

0207 043 7044

hello@stripeolt.com

Bristol

0117 974 5179

hello@stripeolt.com

1 World Economic Forum Risks to Doing Business 2019

2 Names have been changed

3 The risk-based approach to cyber security, McKinsey, October 2019

CYBER SECURITY TOOLS FOR EVERY BUDGET

The good news is that the software tools required to run a business have become cheaper, easier to use and more accessible. The security tools your business needs are no exception, with many available as standard through your Office365 subscription.

Secure Score

Secure Score allows you to measure the security of your infrastructure, and then benchmark it against other Office365 users to understand your progress in context. It also flags up potential risks before they become issues, and reassesses scores as new threats emerge.

Office 365 Advance Threat Protection (ATP)

ATP monitors email traffic to flag up phishing attempts, malicious content such as viruses or malware, and verifies links to ensure that they lead to benign locations.

Multi-Factor Authentication

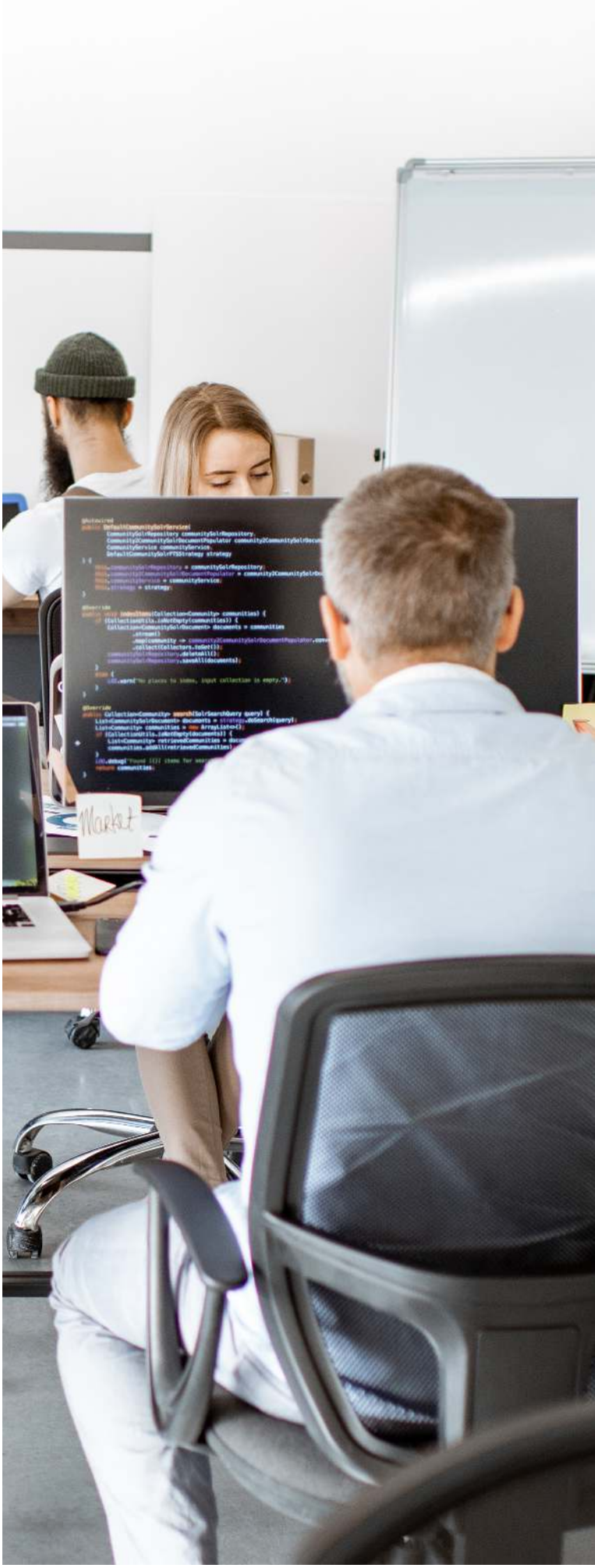
Combine login credentials with one-time codes sent to a personal device to make it impossible for a bad actor to use compromised passwords to gain access to your systems. MFA is simple, effective and easy to deploy.

Attack Simulator

How would your people react when faced with a phishing email? With Attack Simulator you can create realistic-seeming malicious emails to send to your organisation, and then monitor the resulting activity. This allows you to identify teams or individuals who might need additional training.

Data Loss Prevention (DLP)

A great example of risk-based protection, this tool allows you to categorise information according to its sensitivity and retention requirements. You can then apply different rules for sharing and encryption to each category, including triggering alerts when certain files are sent over email.



London

0207 043 7044
hello@stripeolt.com

Bristol

0117 974 5179
hello@stripeolt.com

MEASURING RISK, NOT ACTIVITY

Changing the way your organisation thinks about security means altering its measures of success. Instead of itemised checklists of security initiatives and tools implemented when budget allows, every organisation of every size should be assessing overall cyber security risk in order to plan its security strategy. Progress can then be measured on how far this risk has been reduced, rather than on initiatives achieved with no consideration of their overall impact.

Factors to consider in an overall risk assessment range from the types of information and data the organisation holds (and who owns it), to how employees access and work with information such as emails or documents, infrastructure, hardware and software, and crucially the potential impact of a data loss, breach, or other security incident. In the UK, the government's Cyber Essentials and Cyber Essentials Plus schemes (see separate box) offer a useful starting point for organisations to start their security assessments and remedy some of the most common issues.

"Having Cyber Essentials certification is increasingly becoming a requirement from our own clients," says Brendan, partner in an architectural firm. "It's a good way of knowing that an organisation is taking cyber security seriously."

CYBER ESSENTIALS, CYBER ESSENTIALS PLUS & ISO 27001

The Cyber Essentials scheme was developed to show organisations how to protect themselves against low-level "commodity threat." It lists five technical controls that organisations should have in place:

- Access control (who can log in to which systems)
- Boundary firewalls and internet gateways (what points of entry exist on the system)
- Malware protection (detecting and blocking viruses, dodgy links and files)
- Patch management (ensuring all systems are maintained with the latest software updates)
- Secure configuration (setting up systems in the most secure manner possible)

The vast majority of cyber attacks use relatively simple methods which exploit basic vulnerabilities in software and computer systems. There are tools and techniques openly available on the internet which enable even low-skill actors to exploit these vulnerabilities. Properly implementing the Cyber Essentials scheme will protect against the vast majority of common internet threats.

While the basic Cyber Essentials scheme focuses on policies and procedures, Cyber Essentials Plus focuses on the health of your network, and includes a vulnerability scan by an accredited tester.

ISO 27001

For organisations where security is an intrinsic part of their service offer, the ISO 27001 international standard helps organisations manage their information security processes in line with international best practice.

London

0207 043 7044

hello@stripeolt.com

Bristol

0117 974 5179

hello@stripeolt.com

WHAT IS YOUR GREATEST RISK?

Measuring overall risk requires an understanding not just of current active threats and an organisation's vulnerabilities, but also of the risks inherent in a particular sector or industry.

For example, PwC found that "85 percent of airline CEOs expressed concern about this risk [cyber security] versus 61 percent of CEOs in other industries, a difference of 24 percentage points." [4]

Some of this is down to the types of systems required by different industries: on top of the the usual concerns about information theft or data leakage, airlines need to manage extensive operational infrastructure to keep their planes flying. Where companies in one sector all use a common system, such as Air Traffic Control, the risks broaden out to include the ones posed by links to other stakeholders.

But even in firms running less complex systems, an understanding of the risks particular to an industry can be useful:

"Attackers are becoming more and more sophisticated," says Daniel. "For example, they know that most completions for house purchases, which involve large sums of money, go through on a Friday. So they often target law firms on that day."

RISKY PEOPLE

Any risk assessment should also consider the fact that one of an organisation's greatest vulnerabilities is its people. Attackers know that targeting people in the hope that they might make a crucial error is far simpler and cheaper than trying to hack into secure systems, so the most common forms of cyberattack are simple phishing expeditions.

"We understand as much as anyone that security technology is only part of the solution," says Martin. "A lack of attention to detail, or not following procedures by one of our people can leave us open to being hoodwinked by outside operators."

"The biggest risk when it comes to an organisation's people is a lack of awareness," explains Tom Robbins, one of our Stripe OLT directors. "Cyber attackers have become more sophisticated at mimicking genuine emails and fooling people into bad decisions. For example, attackers use LinkedIn to target specific people inside an organisation who might have access to financial systems. They might also research a company's suppliers or partners in order to pose as genuine contacts."

A recent survey of Chief Information Security Officers by Forbes and Fortinet [5] supports this view: "one of the most clear moves [CISOs] can take to improve their organisation's overall security posture is to prioritise employee training and create a proactive cyber security culture."

London

0207 043 7044

hello@stripeolt.com

Bristol

0117 974 5179

hello@stripeolt.com

4 PWC - Aviation perspectives 2016 special report series: Cyber security and the airline industry

5 CSO - Putting Your Employees at the Center of Your Cyber security Strategy

WHAT IS A PROACTIVE CYBER SECURITY CULTURE?

An organisation's cyber security culture consists of the knowledge, beliefs and perceptions about cyber security that are held by its people, and their impact on behaviour. For example, if your people believe that cyber security is the IT team's responsibility alone, or that your organisation is too small to be targeted, this will foster a casual approach to actions such as sharing bank details or clicking on links that come in via email. A proactive cyber security culture, on the other hand, is one where each employee takes personal responsibility for keeping the organisation secure, and works collaboratively with others to achieve this objective. The key is for every employee to understand that they, no matter how junior, lacking in wealth or in authority, are a potential target. Not only that, but hackers often use highly personalised emails to exploit people's fears or vulnerabilities, featuring links to divorce papers, for example, or threatening to expose people's activities on porn sites that they claim to have recorded:

"Criminal organizations are compromising legit sites and using those to send legit (and despicably personal) phishing attacks to install malware or ransomware. Often they want to compromise your employer or steal your accounts, because those are extremely valuable for doing more crimes. More to the point, thinking that you're not a target for any reason ("I'm not that interesting" or "I don't have followers/money" or "my job is boring") is going to make you the perfect target." [6]

"We focus on educating our people and making security part of the conversation," says Martin. "We always discuss security to raise people's awareness of the threats out there, and ask people how they're doing at every opportunity."

"At the same time, we must never lose sight of the fact that our systems are here to enable people to do their jobs" continues Tom Robbins. "So while it's frustrating that they are often the weakest link in terms of security, the systems need to work for and with an organisation's people, not against them."

Daniel agrees: "Constantly with IT systems one strives for ease of use and accessibility, and those things are not necessarily fully compatible with security. It's like having a completely secure house – it might be secure, but it's not very liveable. We try to make these systems both liveable and usable."

This means recognising that "technical cyber security measures do not exist in a vacuum, and need to operate in harmony with other business processes to avoid employees being placed in the untenable position of being forced to choose between 'doing their job' or 'complying with security policies'." [7]

Getting this balance right can result in employees becoming a 'human firewall', rather than a weak link. ENISA, the European Union Agency for Cyber security, recommends starting with understanding current beliefs and behaviours around security in order to identify what needs to change. [8]

London
0207 043 7044
hello@stripeolt.com

Bristol
0117 974 5179
hello@stripeolt.com

6 Engadget - Phishing scams leveled up, and we didn't
7 Enisa - Cyber Security Culture in organisations
8 Enisa - Cyber Security Culture in organisations

NOT ALL RISKS ARE CREATED EQUAL

The final piece of the puzzle when considering cyber security risk is to understand that the risk is not evenly distributed across your people. While anyone in an organisation can be guilty of clicking on a dubious link or having a lax attitude to password management, the impact of such a breach can vary enormously.

Tom Robbins says “Categorising your people by factors such as the role they do and the amount of authority and access they have can help you, not only target training where it will be most useful, but also to have a strategic approach to how you manage access to your systems.”

Some typical role-based assessments might include:

THE FREELANCER

Companies are increasingly relying on freelancers and contractors to meet workload peaks, but a key risk is not removing The Freelancer’s access in a timely fashion once the job is complete. Having a specific, firewalled part of your infrastructure dedicated to sharing project-specific information with temporary staff, and ensuring that all access is time-limited, can mitigate the risk of accidental (or deliberate) breach.

THE ACCOUNTS ASSISTANT

While an Accounts Assistant might be in a relatively junior role, her access to financial systems makes her particularly vulnerable to phishing attacks or password breaches. Training, security processes and mandatory password management can help keep Annie’s access secure.

THE ADMINISTRATOR

Assessing the risk from administrators requires assessment at an individual, role-specific level. Personal assistants to executives, for example, may have levels of access far in excess of their seniority in the organisation, and they often have system permissions that allow them to manage their line manager’s email and/or files.

THE IT TEAM

Never overlook the risk from IT staff themselves. While they should be well-educated about the risks, they are likely to have full administrator access to crucial systems and files and are therefore a key target for attacks.

SENIOR MANAGEMENT

Management staff are generally extremely busy and not focused on considering cyber security risks. They often delegate their access to systems and infrastructure to others, which increases their risk profile. Added to this, their level of authority means that spoof emails purporting to be from them and requesting changes to bank details (for example) are less likely to be questioned.

THE CHAIRMAN & NON-EXECS

Part-time directors have significant authority but may have access to a number of different companies’ systems and infrastructure simultaneously, which can pose a risk. This risk is increased if they frequently use their own devices and hardware to connect to your systems.

BUILDING A GREAT SECURITY CULTURE THROUGH RISK MANAGEMENT

The good news is that taking a risk-based approach to your security can have the additional effect of building a great security culture. According to McKinsey, the key to taking this approach is not to treat the enterprise as a single point of risk, but to identify its greatest sources of value. These often generate the most significant risks to the organisation, so can be prioritised from a security point of view. Combining this analysis with an understanding of the key vulnerabilities of your people and your infrastructure then provides a more nuanced picture of where to focus cyber security efforts.

In order to do this, security teams need to work closely with individual teams and departments to identify and map their sources of value and risk. This in itself helps to move the responsibility for cyber security from 'the IT team's problem' to a shared one.

"Making this connection between the cyber security team and the businesses is a highly valuable step in itself. It motivates the businesses to care more deeply about security, appreciating the bottom-line impact of a recommended control. The approach is far more compelling than the maturity-based approach, in which the cyber security function peremptorily informs the business that it is implementing a control "to achieve a maturity of 3.0." [9]

9 The risk-based approach to cyber security, McKinsey, October 2019

London
0207 043 7044
hello@stripeolt.com

Bristol
0117 974 5179
hello@stripeolt.com

INCIDENT CASE STUDY 1
SPEAR PHISHING

In this highly targeted attack, the HR Director's email credentials were compromised. Having identified that the email account was a delegate for other email accounts, (i.e. could send email on others' behalf) the attacker bided their time, monitoring the email traffic in and out of the account.

When they saw that a sizeable payment was due to be made, they sent an email, posing as the Sales Director, with new bank details. They then redirected all responses to the online archive so that the real Sales Director did not see them. This meant they could ensure the payment was sent to their fraudulent account.

How would a good security culture have helped?

A combination of technology, processes and employee awareness could have prevented this attack succeeding:

Multi-factor authentication (requiring a password and a security code sent to a personal device to log in to crucial systems) could have prevented the attacker gaining access to the email account in the first place.

Employees using password management software to ensure that all logins have separate complex passwords would have prevented a password compromised elsewhere being used to gain access to the email account.

Employees in both teams being aware of the high risk associated with the communication of bank details, and following a process where the details are confirmed on more than one channel, would have stopped the payment in its tracks.

Office365 can also be set up to trigger security alerts on emails containing information such as bank details, involving the IT security team at an early stage.

INCIDENT CASE STUDY 2
MALWARE

In this incident, a user received a highly targeted email containing plausible content and an attachment containing malware. When clicked, the attachment triggered the malware, which was able to harvest usernames and passwords to give the attacker access to key system resources. The attacker installed ransomware which locked the organisation out of its data, including 75% of its backups. In the end, the entire network had to be rebuilt from scratch.

How would a good security culture have helped?

Again, a combination of technical systems and user education could have prevented this attack:

Advanced Threat Protection could have prevented the email ever reaching its target user by identifying the malware and alerting the security team.

Identifying the user as high-risk and not allocating administrator rights would have limited the attacker's access.

Identifying the backups as an important source of value in case of an incident, and moving them to a location not accessible through a normal user name and password, would have prevented the attacker wiping them out.

RISK - HOW WILL YOU MANAGE YOURS?

No matter how sophisticated your security systems, enabling people to work effectively and productively inevitably creates security risks. The responsibility for identifying and mitigating the risks always lies squarely with the organisation to initiate and implement, but one of the most powerful tools at any organisation's disposal is to ensure that all its people are aware of the risks, and vigilant about the different forms of attack.

Cyber Essentials and Cyber Essentials Plus are an excellent starting point on any organisation's security journey, helping them to put in place a risk-based and holistic approach to cyber security management.

If you would like to discuss any aspect of your organisation's cyber security, including how to achieve Cyber Essentials certification, please contact our experts directly at hello@stripeolt.com or call us on 0207 043 7044.

CYBER SECURITY SERVICES AT STRIPE OLT

Cyber Essentials & Cyber Essentials +

Cyber security is essential in today's digital landscape and any business can be at risk, which is why it pays to protect your organisation through the government backed, industry-supported Cyber Essentials scheme.

Phishing Simulation & Awareness Training

Prevent and protect your business through practical phishing attack training sessions.

Vulnerability Assessments

Define, identify and classify vulnerabilities in your computer systems, applications and network infrastructures.

Cyber Security User Education

With our tailored courses you can turn your workforce into your first line of cyber defence, with prevention through education.

Penetration Testing

Through robust penetration testing, carried out by our certified experts, discover how cyber-criminals could gain access your business systems and network.

Security Operations Centre

Stripe OLT's dedicated security operations department leverage cutting-edge Microsoft detection technology and artificial cyber intelligence, to offer an unparalleled outsourced SOC service. We provide enterprise-level threat detection and incident response capabilities, without the corporate price tag.

Gold Microsoft Partner

Cyber Essentials Certified Plus

CREST

ISO 27001 Information Security Management

IASME Governance

London
0207 043 7044
hello@stripeolt.com

Bristol
0117 974 5179
hello@stripeolt.com

London

0207 043 7044

hello@stripeolt.com

Bristol

0117 974 5179

hello@stripeolt.com