SOLACE CYBER

PROACTIVE CYBER SECURITY

Optimise your security posture against cyber risks

PROACTIVE CYBER SECURITY

How to get your organisation to good

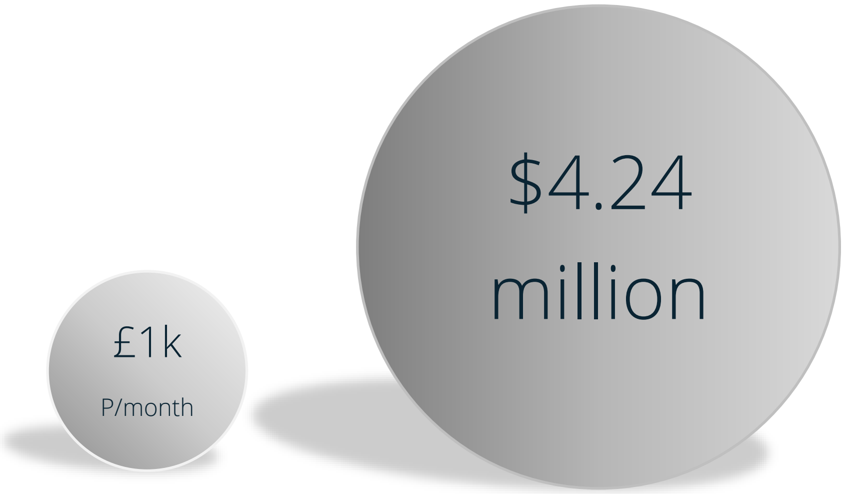
WHAT IS PROACTIVE CYBER SECURITY?

Proactive and reactive strategies are two different approaches when responding to cyber attacks. Reactive cyber security involves an organisation reacting to a cyber security incident post exposure in order to restore business-as-usual. Proactive cyber security is a preventive strategy and focusses on stopping cyber threats before they cause damage. The effective implementation of a proactive cyber security strategy significantly reduces risk and therefore diminishes the likelihood of a security breach. Proactive cyber security means investing in preventative measures, to avoid substantially higher costs in the event of a security breach, to regain business operability.

Average cost of proactive security

vs

Average cost of data breach



Average Solace Global cost <100 users

IBM cost of data breach report 2021

Many organisations assume that the likelihood of being subject to a cyber security breach is improbable, and even if they are breached there is coverage in the form of cyber insurance. This article details why it is imperative for organisations to adopt a proactive cyber security strategy, rather than taking a 'watch and wait' approach.

Cyber security attacks grew significantly in 2021, with the growth curve following a similar trajectory in 2022. Global cyber-attacks were up 29% in 2021, with ransomware attacks up 93% in Q1 and Q2 2021 compared to the same period in 2020, according to Check Point's mid-year security report.

Phishing attacks were also up in 2021, and leading global email security vendor Mimecast's research has shown that 47% of phishing attacks resulted in an account being compromised and 49% of phishing attacks result in malware infection. One reason for increasingly successful attacks is due to phishing emails becoming even more sophisticated, making it much harder for employees to spot a rogue operator.

Solace Cyber Security Incident Response Team (CSIRT) has been at the frontline fighting the attackers and have seen first-hand the catastrophic operational damage, reputational damage and costs that these organisations are facing. Even when cyber insurance is in place, companies are still facing significant unexpected costs from uncovered items, or even more concerning, if the cyber insurance has unknowingly become void due to alack of proactive security protection or compliance to the security terms and conditions within their policies.

EXAMPLE: MARTIN IN ACCOUNTS AND THE PHISHING EMAIL.

Martin is exceptional when it comes to looking after the company's finances. He is always keen to ensure invoices never go undocumented, so when an unrecognised remittance email came through with an attachment – he was keen to check nothing had been missed by the team and saved the attachment on his PC.

It is in this instance an email has successfully infiltrated the mail flow protections. From here, two things are likely to happen:

1. When clicking on the link that is embedded within the email text, macros and automation will kick into life, which downloads malware onto the employee's device.
2. The employee will be taken to a webpage whose sole purpose is to harvest their username and password, this spoof webpage will request the employee's corporate login credentials which many employees unwittingly enter by mistaking the webpage for a legitimate service (e.g. www.office.com)

When a malicious party has the employee's username and credentials they will attempt to login to their account. If access to the account is obtained, they initiate multiple attack vectors. Firstly, mail rules will be put in place to ensure all their activity is hidden from the employee. The contents of the emails will then be reviewed, gaining substantial information to help them in deciding what to do next. When there is lots of personal data available that is highly valuable to them, the data will be extracted or forwarded outside the organisation, to either sell on the dark web or initiate identify theft scenarios. The attackers may also send mass outbound malicious spam emails from the compromised account, with the aim of compromising other staff or your clients. Another alternative attack method is to edit invoices and modify bank account details, before sending fake invoices to your clients to obtain fraudulent payments. They may edit emails and have fake conversations with your clients and other employees, again leading to fraudulent situations.

THE POTENTIAL COSTS FROM A SUCCESSFUL PHISHING ATTACK

So, we now understand some of the risks of a simple successful phishing email. Time to highlight some of the costs...with GDPR changes and the Information Commissioner's Office (ICO) in place, the loss of personal data (PII/PFI) is considered high risk and will trigger a 72-hour legal obligation to notify the ICO. In order to understand the risks and correctly complete the ICO submission forms, a security forensic team is often required to perform an investigation. If the data that has been lost is considered to pose a high risk to the freedoms and rights of the individuals, then a formal notification strategy to the people whose data has been lost will be required. These notification strategies are very detailed in their requirements and must be executed as per the legal guidelines.

A small ICO submission is likely to cost from £5k to £25k, and a large ICO submission could cost upwards of £100k. Solace Cyber has seen organisations face charges in excess of £1 million in notification costs, not including the cost of reputational damage to a company from which some organisations never fully recover. There have been some very public instances where the ICO or GDPR requirements have not been met sufficiently and large fines have been issued. Some of the largest GDPR fines are referenced here. British Airways is referenced in this list after being fined €22 million ($26 million) following a mishandled security breach.

After experiencing a breach of this nature, the ICO will ask you to reference how and what your organisation will be doing to ensure that a similar breach does not occur again. These costs and security measures will then become an obligation. If another breach should occur and these improvements cannot be evidenced to the ICO, this will cause further complications for your organisation.

Often organisations argue that cyber insurance will cover all of these costs, but this is not always the case. Typically, cyber insurance will cover any loss incurred during the incident and up to the point of full recovery, however there will be additional investment required to satisfy the ICO and prevent another breach, which will be a cost that an organisation has to swallow.

FACTORS THAT CAN AFFECT YOUR INSURANCE COVERAGE

It is important to check against your terms and conditions;

- ✓ Does your insurance cover data loss?
- ✓ Do you have end of life systems or unpatched systems that may void your insurance?
- ✓ Does your data loss policy include notification coverage costs?
- ✓ Is your firewall patched to the frequency set out in the policy?
- ✓ Are there any other mandated actions (e.g. employee phishing awareness programmes, ongoing vulnerability assessments)?

By not meeting cyber insurance terms and conditions, Solace Cyber has seen many organisations facing all of these costs themselves, in addition to significant reputational damage from a single phishing email.

The above has referenced the risks of harvesting credentials but equally the malicious payload downloaded when the phishing link was clicked could spread into the network and download a dormant ransomware package. Ransomware became much more advanced during 2021 and has the capacity to steal all of your company data, before encrypting the business. This can leave your company inoperable, unless the data can be recovered in some way from backup, or by paying a ransom to the attacker. If the data cannot be recovered by either means, this could mean rebuilding the entire business or going into liquidation. The cost of recovery is much greater for organisations that have not taken proactive cyber security measures.

HOW PROACTIVE CYBER SECURITY PREVENTS A BREACH

Solace Cyber have recommend a number of key functions and configurations, designed to be both simple and cost effective to businesses:

- Firstly, mail flows can be security hardened which can significantly reduce the chance of a phishing email arriving to the employee in the first instance. Security hardening and alerting to an expert level can be actioned within a few days. This could reduce successful phishing arriving at the employee by 90%.
- Monthly phishing simulations and cyber education can cost as little as £2 per user per month. This can provide all of the tools the employee needs to not click the phishing email or provide their credentials.
- Multi Factor Authentication (MFA) – you may already have the licences for 2FA which can be implemented very quickly. If the employee provides their credentials, the attackers would also need to have stolen their pervasive device or convince the employee to bypass their MFA.
- Endpoint Detection and Response (EDR) – is a very cost-effective way to kill the malicious payload processes from a successful phishing email, before it can spread. This technology can prevent the

ransomware scenarios, isolate the compromised devices and can be monitored 24/7/365 by a SOC team.

- Remember, cyber insurance will not cover for additional technological and operational measures deployed post recovery. Therefore, its best to invest in these upfront, to proactively reduce future costs before a first breach occurs.

CONCLUSION

If we take a SMB business with <100 employees as an example, the proactive security protection highlighted above might cost £1000 per month or around £12k per year. One single employee clicking a phishing email might cost this organisation £100k + in a breach recovery scenario.

When Solace Cyber run an initial phishing simulation against an organisation, the average failure rate in that first simulation is 25%. By reducing the number of employees that fail the test, you drastically reduce the risk to your business operations due to a successful phishing email.

Solace Cyber are specialists in both reactive and proactive cyber security. We have helped many organisations recover following a cyber attack. The sentiment amongst all breached organisations is that they wish proactive security strategies and solutions were put in place sooner.

Learn more about proactive cyber security measures

Discover free resources and risk assessments, to help identify your organisation's cyber security position.

- Learn more about how not to void cyber insurance
- Book a free of charge Cyber Risk Assessment

Contact our cyber risk management specialists today

cyber@solaceglobal.com

+44 (0)1202 308810