CLEARSWIFT
ADAPTIVE CYBER PROTECTION

A THREE POINT PLAN ENSURING A ROBUST IT SECURITY POLICY

Covering social media, third parties and your security

No man is an island and no company is either. Confidential information is regularly exchanged with business partners and communications with the outside world are now less manageable due to social media. Here's how to tackle the issue before it tackles you.

STEP 1

Investigate how people communicate within your organization using digital channels (such as email, Skype, Twitter, Facebook, LinkedIn etc.) and devices (such as laptops, tablets and smartphones)

WHO ARE YOU COMMUNICATING WITH?

Who are your staff talking to as they undertake their daily roles?

SUPPLIERS? PARTNERS? THE PUBLIC?

WHY ARE YOU IN CONTACT WITH THEM?

What's the purpose of the communication? Is this something urgent or not? What's the information being shared? Do they have the authority to share this information?

For example, is social media used to make company announcements and topical comments?
Is email being used to transfer personal data?

HOW ARE YOU COMMUNICATING WITH THEM?

50% of public sector organizations are concerned that social media channels could pose significant risks to their IT security.

TO BYOD OR NOT TO BYOD?

If you are subscribing to a 'Bring Your Own Device' policy, appropriate use of these devices must be allowed for an organization's IT security. You should also consider what happens to the data on these devices when the employee leaves the organization.

WHAT ARE YOU COMMUNICATING?

Do you know what the information being communicated is? Does it contain confidential information?

10% of public sector organizations do not consider information security to be important when selecting a business partner

84% of information exchanged with third parties is sensitive.

WHO IS DOING THE COMMUNICATING?

Not everyone in your organization needs access to all data - or the right to communicate this data. You may find that you require layers of security, meaning, for example, the CEO can view an entire report, whereas people further down organization only have access to what is relevant to them.

STEP 2

Investigate what security policies are in place to deal with communications and whether they are being enforced.

WHAT DOES YOUR SECURITY POLICY COVER?

Has it been updated to include all social media platforms, staff's own devices and third parties?

38% of public sector organizations do not have an organizational strategy in relation to their outbound communication technologies.

HAVE YOU CONSIDERED ACCIDENTAL, AS WELL AS MALICIOUS, SECURITY INCIDENTS?

What happens if an email is sent in error or a disgruntled employee tweets from the corporate account? What procedures are in place to deal with this?

ARE YOU PASSWORD SECURE?

How often do you change the passwords on your corporate social media accounts and are they complex enough to stop hackers? Who has access to them internally?

DOES YOUR POLICY MEET LEGISLATIVE GUIDELINES FOR YOUR INDUSTRY SECTOR?

Break these rules and you could be setting yourself up for a fine.

HOW IS YOUR POLICY CONVEYED TO YOUR EMPLOYEES?

An untrained employee is a security risk for the whole organization. Explaining the IT security policy should form part of every employee's induction.

HOW OFTEN DO YOU REFRESH YOUR EMPLOYEE'S KNOWLEDGE OF THE SECURITY POLICY?

Whether your security policy changes or not, employees need to be reminded of it. Time spent on this will save money spent of rectifying incidents, as well as avoiding any reputational damage.

Fire drills must take place every year, despite the low chances of a fire actually occurring. Security policy refresher courses should take place every few months.

STEP 3

WHAT ARE THE CONSEQUENCES OF GETTING IT WRONG?

31% Reputational damage to the organization

20% Financial consequences

18% policy or compliancy issues

HAVE YOU GOT A PLAN FOR WHEN SOMETHING GOES WRONG?

Let's face it, something will go wrong...
Do you know who will be in charge, who will communicate on behalf of the organization with the media, customers (citizens)?

WHY IT PAYS TO BE SECURE

MONEY · REPUTATION · COMPLIANCE · PEACE OF MIND

WWW.CLEARSWIFT.COM