CYBER PROTECTION

A bespoke collaborative solution to mitigate and protect against emerging cyber threats

RSA

INFORMATION TECHNOLOGY REVOLUTION

Most organisations have a critical reliance on information technology to conduct their business. In fact, over a relatively short period of time we have lived through a revolution that has seen every aspect of our lives affected by the generation, transmission, storage and analysis of vast amounts of data (both personal and commercial) and a reliance on the infrastructure (both tangible and intangible) that supports it.

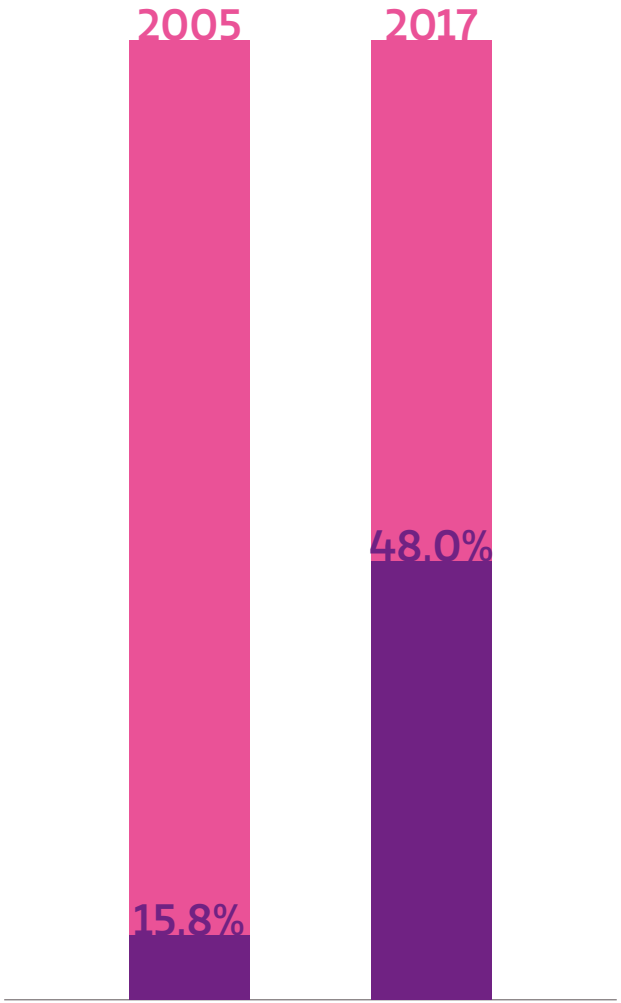
This Information Technology (IT) revolution has produced many benefits, however, some of the characteristics that make it so powerful – remote access, scalability, processing power and anonymity – are also the reasons why it has proven to be a lucrative arena for criminals to operate in.

Malicious activity is only part of the problem. We are all prone to making mistakes from time to time and when we do, human error has the potential to affect critical IT infrastructure and the impact can be catastrophic.

1 MILLION PIECES OF MALWARE ARE CREATED EVERY DAY

Source: Microsoft

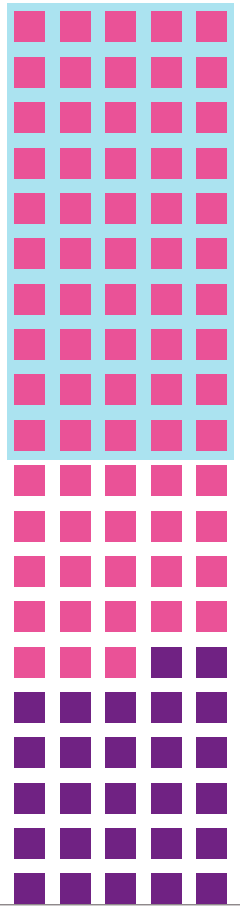
From 2005 to 2017, the percentage of the global population using the internet increased by over 32%



Source: data.worldbank.org

THREAT ACTORS AND THREAT VECTORS

In 2017, 73% of breaches were perpetrated by outsiders, including 50% that involved organised criminal groups



50%
of breaches were carried out by organised criminal groups

73%
of breaches were perpetrated by outsiders

27%
of breaches were perpetrated by insiders

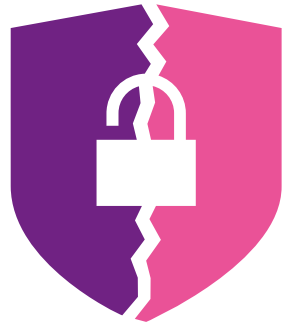
Source: Verizon DBIR

Most cyber events are caused by malicious actors (be it internal or external) but this is closely followed by non-malicious actions such as human error and unexpected technical failures. The picture becomes more complex when you consider the increasing activity of nation states employing cyber warfare.

These threat actors use a large number of methodologies - or 'threat vectors' - to achieve their aims. Methodologies range from simple phishing scams to gain log on credentials to advanced persistent threats (APT) that are engineered to disrupt critical national infrastructure. Threat vectors evolve as rapidly as the technology they exploit, making the task of implementing a comprehensive information security management system (ISMS) increasingly difficult, even for large sophisticated organisations.

48%
of breaches last year involved hacking

Source: Verizon DBIR



RISK MITIGATION

Good cyber hygiene is essential to mitigate the risks and is the core of much advice, for example the Cyber Essentials Scheme supported by the UK Government. However, larger organisations will need to follow a comprehensive information security management system, such as that proposed by National Institute of Standards and Technology (NIST) or the ISO 27001 series of standards.

In addition there are a range of other industry standards, for example the Payment Card Industry Data Security Standards (PCIDSS), that must be followed by companies deploying point of sale devices and transacting debit and credit card payments. The general belief is that a properly deployed ISMS (information security management system), combined with good user awareness, can defeat the majority of cyber incidents.

LEGISLATION AND REGULATION

The Seven Data Protection Principles*:

*as set out in the GDPR guidelines

The General Data Protection Act 2016/679 (GDPR), which came into force on 25th May 2018, is a milestone in the development of data protection law and enshrines fundamental rights for individuals in the European Union in respect of their personal data, no matter which company holds it or in which country it is held. The GDPR is part of a global legislative drive to put individuals in control of their data, encourage organisations to protect it and hold them liable if they do not. Laws with similar provisions are now in place in many countries around the world.

May 2018 also saw the Network and Information Systems (NIS) Directive being enacted into UK law. One of the key objectives of the NIS Directive is to ensure that Operators of Essential Services (OES) take appropriate and proportionate technical and organisational measures to manage the risks to the security of network and information systems which support the delivery of essential services. They are now required to meet a set of 14 NIS cyber security principles.

The regulatory landscape has evolved to keep pace and there are now dedicated information or data commissioners in most jurisdictions. They have significant powers to investigate and, ultimately, fine companies that fail to abide by the law.

Organisations that collect, process or store personal data, or provide essential services, now operate in an environment where a failure to manage that process properly is increasingly likely to result in significant financial and reputational damage.

BUSINESS IMPACT

A cyber event can have a variety of impacts on a business, more so perhaps than is immediately obvious, and all have cost implications which can be significant;

- Costs for notifying those affected
- Credit monitoring and identity theft insurance costs
- Legal Advice costs
- Reputation management costs
- IT forensic costs
- Defence costs and damages
- Loss of profit

CYBER PROTECTION
FROM RSA

Cyber Protection from RSA covers all the typical costs associated with a cyber event, but importantly it also provides a 24/7 incident response capability* that supports and enhances an organisations own crisis management and response capability. **We can provide capacity up to a limit of £25m and our policy offers worldwide cover.** The policy provides the following coverage options;

- **Data liability**
- **Network security**
- **Multimedia liability**
- **Regulatory costs, fine and penalties**
- **Cyber business interruption**
- **Contingent business interruption – named suppliers or unnamed suppliers**
- **Payment card industry expenses**
- **Cyber extortion**
- **Payment diversion fraud**
- **Breach response: Confidentiality, Integrity and Availability costs**
- **Communication advice and support**
- **Emergency costs and expenses**
- **Mitigation costs**
- **Strategic advice for your senior teams**
- **Crisis management office support**

We can also offer risk assessment support by our partners Deloitte. This enables us to undertake a detailed risk assessment prior to binding the insurance policy, which directly benefits our customers as they will be provided with a copy of the assessment findings which can then be used in their own risk management process.

Deloitte can help you be better prepared to respond and recover from any cyber crisis by having the right structure, people, plans and playbooks in place. And in the event of a cyber-crisis, you can call on Deloitte's expertise in a number of ways, including crisis communication and reputation management support.

***The 24/7 incident response capability is supported by our partners Crawford & Company.**

OUR PARTNERS

We partner with leading providers to ensure that our customers enjoy best in class risk assessment and crisis readiness services provided by Deloitte, allied to a comprehensive 24/7 incident response managed by Crawford, the world's largest publicly listed independent provider of claims solutions, who can access a variety of specialist IT forensics companies, law firms and other service providers offering the full suite of services required for comprehensive cyber response.

Crawford®

http://www.crawco.com

Deloitte.

http://www.deloitte.com

CONTACTS

Please contact us directly on **cyberliability@uk.rsagroup.com** or speak to your broker to find out more about our cyber proposition.

UKC05144