Grant Thornton

An instinct for growth™

Cyber security

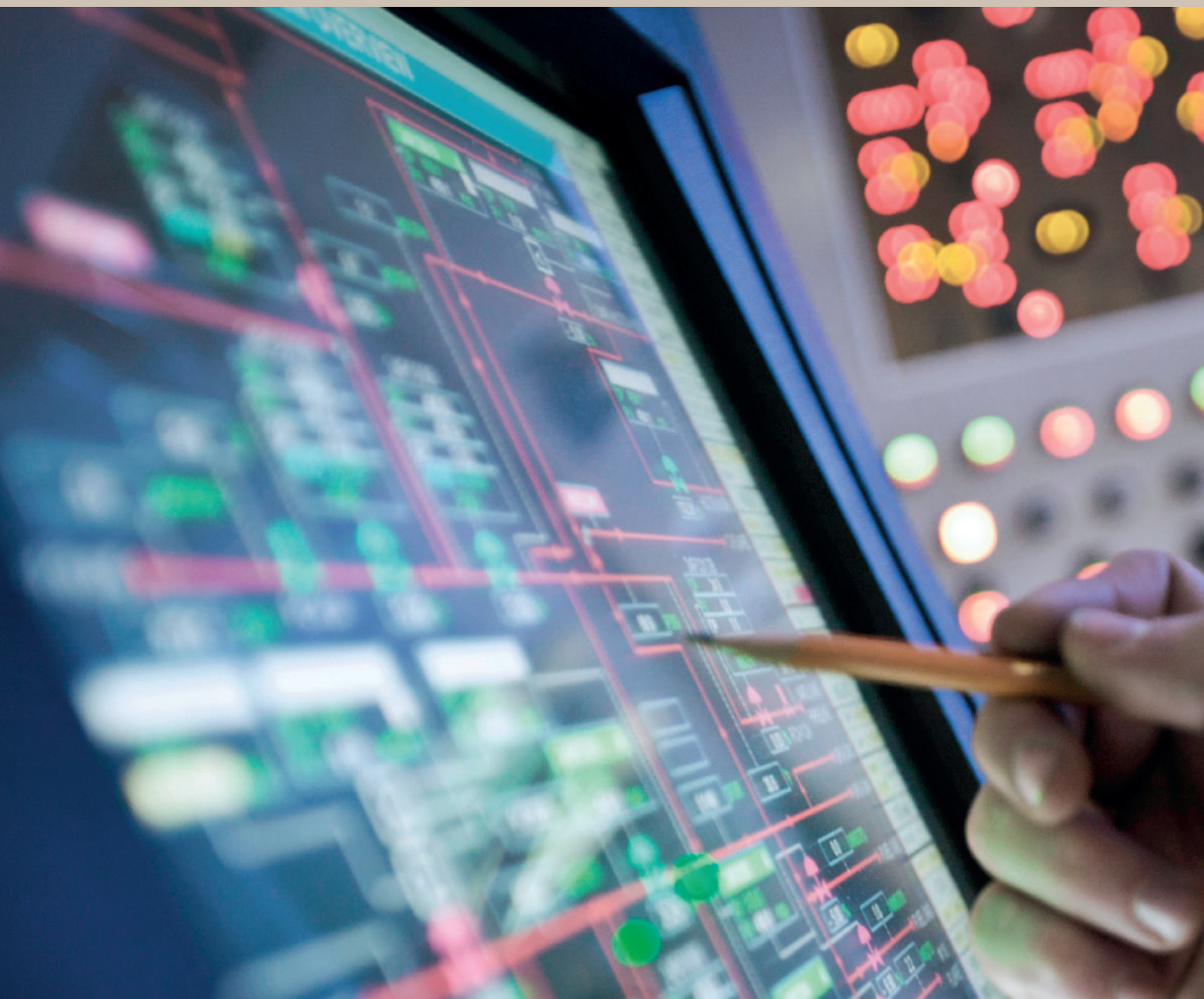
Advisory

Risk

Cyber-crime: avoid paying the price

Protecting your business

Contents:



Executive summary

Getting to the heart of cyber risk

Senior leaders face an array of ever-increasing complex, interconnected and fast-evolving risks and challenges.

Few of these are as critical and so poorly understood as the risk of cyber-crime, specifically given that real life and online are becoming increasingly indistinguishable from each other.

Attacks against businesses and nations occupy the headlines with such regularity, that the estimated cybercrime damage prediction of $6trillion annually by 2021[1] is no longer astonishing. The cybersecurity community and main media outlets have largely concurred with these predictions which have increased, up from $3 trillion just a year ago[1], therefore it is innocuous to say that cyber-theft is fast becoming the largest weaponless crime in the world.

As the world goes digital, humans have moved ahead of machines as the top target for cyber criminals. Microsoft estimates that 4 billion people will be online[1] by 2020 - twice the number that are online now, therefore the entry point for cyber-crime will continue to evolve alongside new entrants to the 'Internet of Things' (IoT).

This trillion-dollar business has multiple facets which include targeted attacks, smartphone threats, social media scams, and IoT vulnerabilities, as well as exploitation of weaknesses in data privacy and infrastructure across a wide range of businesses and industries.

The rising tide of cybercrime has pushed cybersecurity spending on products and services to more than $80 billion in 2016, according to Gartner, this is predicted to exceed $1 trillion over the next five years[1].

Through insights obtained from the Grant Thornton International Business Report[2], alongside the array of data and research available, we explore the global impact of Cybercrime, whilst ascertaining the key fundamentals which owner-managed businesses (OMBs) must apply in order to remain cyber-secure in the future.

"As the corporate world becomes borderless, employees must be aware of the multifaceted issues surrounding cybersecurity, and the necessity for the private sector, government and law enforcing agencies to work in concert to manage the risk of our increasing interconnectivity. When we look closer to home, regional regulators are providing aligned reforms which support innovation, the latest of these include embracing fin-tech and insure-tech, which undoubtedly will not be immune to cyber-crime."

Hisham Farouk
CEO
Grant Thornton
United Arab Emirates

[1] Cybersecurity Business Report by CSO, June 2017
[2] Grant Thornton International Business Report, Q4

The prevalent access points

Real life and online are becoming increasingly indistinguishable from each other, hence the prevalent access points for cyber-crime will continue to grow with the evolution of technology and organisational transformation.

As both individuals and corporates, realism must prevail in terms of the level of exposure which we are unintendedly under, largely driven by our need to enhance efficiency, save time and exploit new technological innovation.

The cyber-criminal has many access points from which they can comfortably attack, we assess the most common as:

- **Smartphones**
- **The internet of things**
- **Web attacks and exploiting vulnerabilities online**
- **Targeted attacks and Intellectual Property (IP) theft**
- **Computers, cloud and IT infrastructure**

The alarming rate at which these access points are being targeted have become a focal point for organisations to consider, not to mention the level of sophistication being applied by cyber criminals.

Smartphones

Globally over 1.4 billion smartphones were purchased in 2015, up 10 percent from the previous year[3], at the same time, mobile manufacturer Ericsson, predicts there could be as many as 6.4 billion smartphone subscriptions by the end of 2020, accounting for almost one per person.

To continue enticing consumers to smartphones, manufacturers continue to lure their consumers with new add-ons or innovative solutions which will drive further efficiency for users by storing all personal data in one place. A simple example of this is the mobile payment system, which allow users to manage their cards in a smartphone wallet, thereby depleting the need to carry cash or cards.

Smartphones are an increasingly attractive target for online criminals. Thus, they are investing in more sophisticated attacks that are effective at extorting valuable data or money from victims.

Organisations can protect themselves by ensuring corporate emails or data are not exchanged via personal smartphones, any such data which is required should be encrypted effectively to protect virtual exploitation.

[3] IDC's Worldwide Quarterly Mobile Phone Tracker
[4] Internet Security Threat Report VOLUME 21, APRIL 2016, Symantec

6.4bn

smartphone subscriptions expected by 2020, increasing the risk of a cyber attack

20.8bn

estimated connectivity from IoT

2tr

estimated economic benefit of IoT

1/3

more than one third of websites are at risk

The internet of things

Internet-connected assets which we use and operate daily are multiplying rapidly. These devices are powerful enough to control our homes, cars and manage our personal and professional lives much more efficiently.

IoT is predicted to deliver $2 trillion of economic benefit, which will see connectivity of things go from 6.4 billion in 2016 to 20.8 billion in 2020[4]. Designers and manufacturers must however address the fundamental security challenges which this level of connectivity brings. IoT devices often lack stringent security measures, and some attackers are able to exploit vulnerabilities in the underlying operating systems found in several IoT devices and routers. Such weaknesses were witnessed by Fiat Chrysler who recalled 1.4 million vehicles after researchers demonstrated a proof-of-concept attack where they managed to take control of the vehicle remotely.

In the UK, thieves hacked keyless entry systems to steal cars, likewise, over 50 commercially available devices, including a 'smart' door lock could be opened remotely online without a password[4], further highlighting the societal but corporate risk that is present.

As IoT gains momentum, we may expect to see cybercriminals using such devices as the preferred route of attacking organisations, which will cause a profound loss, as staff fail to recognise the danger or poor levels of security which such connected devices have.

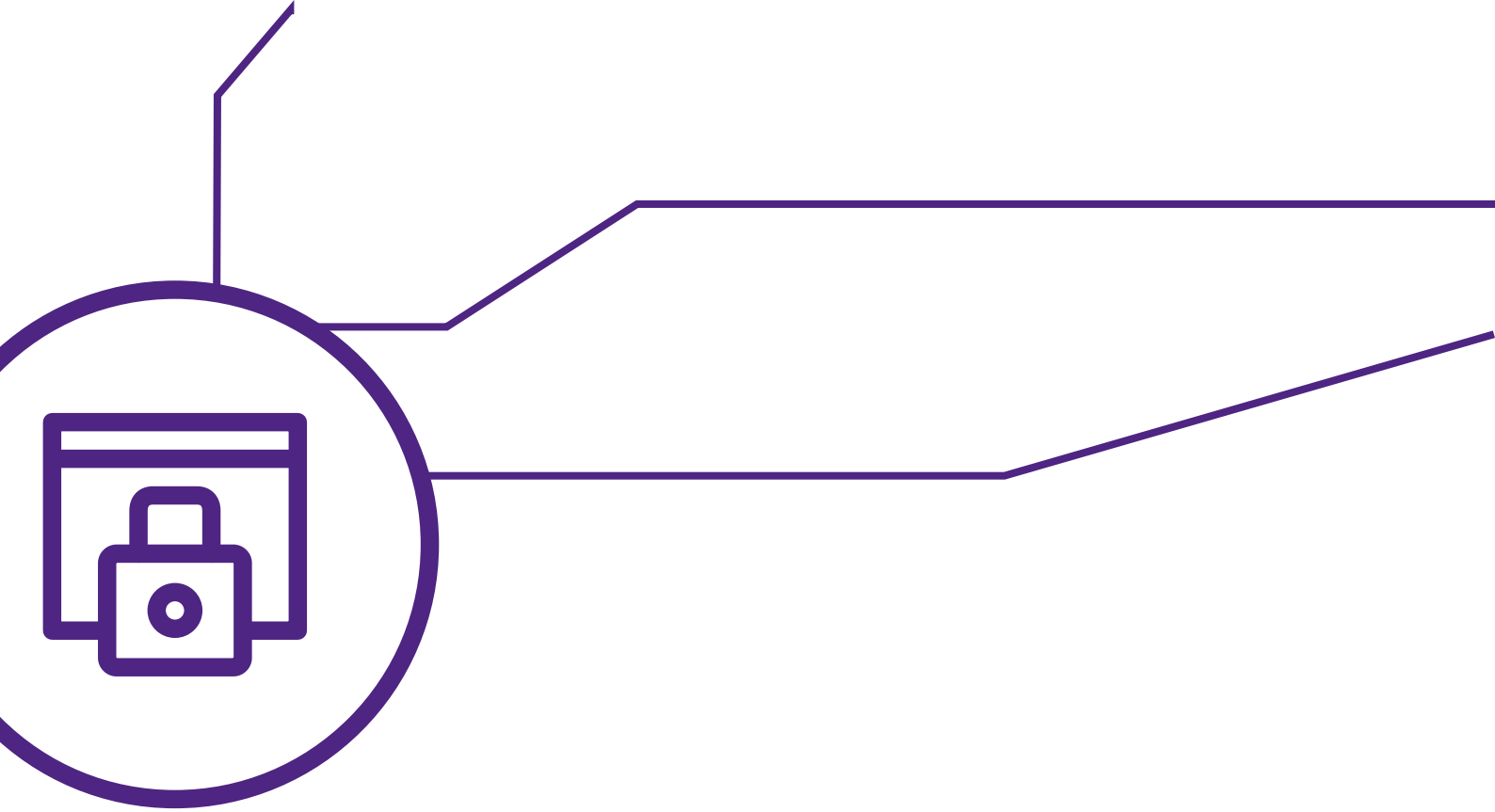
Web attacks and exploiting vulnerabilities online

Vulnerable web servers give rise to exposed websites and those who visit them. Likewise, attackers stop at no means to exploit any vulnerabilities which make exist, resulting in a compromised website and control of the host server.

In there simplest form, many scams still rely on the poor security habits of users to succeed, such as the downloading of malicious attachments from impersonated emails or the use of sophisticated social engineering to bypass the two-factor authentication systems designed to safeguard users. Similarly, the introduction of virtual currency such as bit-coin and the emergence of fin-tech will increasingly add further strain to organisations in respect of protecting their financial and corporate assets.

The sophistication and ruthlessness of some of the attacks and tactics used by cybercriminals have demonstrated how vulnerable we are online as consumers and organisations.

Website owners are not patching and updating their websites and servers as often as perhaps they should, as validated by Symantec, who found that over the past three years, more than three quarters of websites scanned contained unpatched vulnerabilities, one in seven (15%) of which were deemed critical[4].



Targeted attacks and Intellectual Property (IP)

Targeted attacks are becoming stealthier and far more damaging for the organisation under attack. Several recent high-profile cases have illustrated the depth of the crime which exists, alongside the detrimental financial and reputational damage which is caused.

In February 2015, 78 million patient records were exposed in a major data breach at Anthem, the second largest healthcare provider in the US. In the same year, the White House, the Pentagon, the German Bundestag, and the US Government's Office of Personnel Management lost 21.5 million personnel files, including sensitive information[4].

Furthermore, the recent 'Wannacry' attack which affected more than 75,000 systems in 99 countries became the world's largest ever cyber-attack, which disabled large sophisticated organisations such as the UK's National Health Service, several Russian banks and Spanish telecoms operator Telefonica to name a few.

The sophisticated, well-resourced, and persistent cyber-attacks around the world are becoming a reality, which increasingly impact organisations of all sizes and industries. Organisations must ensure they remain protected through the application of the latest software and hardware security updates.

Computers, cloud and IT infrastructure

IT systems continue to be attacked by rapidly evolving malware, coupled with this, operating systems and cloud based solutions are also under threat.

No operating system, whether cloud based or virtual is immune, given Malware has the capability of seeking them out in a virtualised environment and infecting them.

Cloud is increasingly handling and managing more of our data daily, whether it is for customer relationship management, invoicing services, social networking, mobile email, and a whole range of other applications, therefore attackers will look for vulnerabilities which they will be ready to exploit.

Operating systems and applications used are important aspects when considering cybersecurity, likewise businesses must protect their computers and IT infrastructure in order to avoid data loss, theft or system damage, which will undoubtedly have a commercial impact on the business and its customers.

Legal viewpoint

Dino Wilkinson, Partner, Clyde & Co, Middle East

Technological developments have helped many organisations to increase efficiency through digitisation of records and processes. This has also caused an exponential increase in the volume of data being stored and processed by all types of business. As a result, the "surface area" for attacks is significantly larger. Corporate IT systems (and the data they hold) are vulnerable to a range of threats including criminal organisations, disgruntled clients, ex-employees, activists and cyber terrorists. One particular trend in 2017 has been the rise of ransom cases involving demands for the return or decryption of data or to avoid a devastating cyber attack.

Cybersecurity regulations are developing rapidly around the world. The relevant laws typically focus on both deterrence (criminalising specific online activity such as hacking or denial-of service attacks) and prevention (encouraging good information handling and security). The recent global trend has seen governments and regulators introducing new laws or tightening existing legislation to impose more stringent cybersecurity obligations on organisations and higher penalties on cyber criminals.

In Europe, the General Data Protection Regulation (GDPR) and Network and Information Security Directive (NISD) will come into force in 2018. These new pieces of legislation will substantially increase the scope of organisations that will be subject to European cybersecurity laws, potentially including all businesses established in or providing services into the EU. GDPR, in particular, will introduce strict new rules on data security, reporting and breach notification with potential fines for non-compliance of up to €20 million or 4% of annual global turnover (whichever is greater).

The US has a more patchwork approach to data and cyber laws. Regulations typically apply to specific business sectors (e.g. healthcare, financial services, government) in addition to federal legislation on issues of homeland security and anti-terrorism. Certain states have also passed legislation regulating cybersecurity and protection of certain types of data.

The Asia Pacific and MENA regions are two areas where cyber laws are perhaps developing most rapidly and the landscape is constantly changing. India introduced the Information Technology Act 2000 to regulate data protection as part of efforts to improve the framework governing its local IT industry. This was supplemented by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

Elsewhere in Asia, Japan appointed a Personal Information Protection Commission in 2016 to supervise updates to its data protection laws; Australia passed a mandatory breach notification requirement; and China adopted a Cyber Security Law that took effect in June 2017.

In the Middle East, the UAE's Cybercrime Law of 2006 was updated in 2012 to clarify and expand on the scope of cyber offences. While the UAE presently lacks a national data privacy law, there are data protection regulations in the financial free zones of Dubai Healthcare City, Dubai International Financial Centre (DIFC) and Abu Dhabi Global Market (ADGM) that impact companies operating from those jurisdictions.

Qatar became the first Middle East jurisdiction to regulate data privacy at a national level with the passing of the Privacy and Protection of Personal Data Law in 2016; Saudi Arabia has proposed a set of mandatory regulations for cloud service providers intended to address issues including confidentiality, reliability and national security. Bahrain also announced that it expects to pass new laws on data protection and data sovereignty before the end of 2017.

National regulators are constantly monitoring international best practices to ensure that cyber laws are as up to date as possible to safeguard national security, consumer protection and investor confidence. Many emerging markets are taking the lead from other jurisdictions, such as Europe – various regulators are (publicly or privately) considering whether the requirements of the GDPR should become the de facto standard for data protection and we are seeing increasing efforts to coordinate against cybercrime on an international basis.

What can businesses do from a legal perspective to protect themselves from a cyber-attack? All organisations should be assessing the volumes and types of data they hold in order to understand their level of cyber risk. An audit of this nature should also identify where data or systems are shared with other parties and the controls that are in place.

Subsequent risk management measures might include the implementation of privacy policies and a cyber breach response plan; reviewing contract documentation; and ensuring that appropriate information is given to individual employees and customers about the use of their personal data.

In-house lawyers and outside counsel can help businesses to protect against cyber risk, respond to cyber threats and recover from cyber attacks.

Dino is a Partner in the communications, media and technology practice at international law firm Clyde & Co. He has been advising clients on technology-related legal issues for more than 15 years.

The global impact

When we look at the global impact of cyber-crime in numbers, the depth of the crime unfolds. This trillion-dollar business is now one of the largest crimes globally, which is projected to reach a total cost of $6tr by 2021[4].

"Cyber risk is an evolving threat – new technologies and new ways of doing business create opportunity but can also be a source of risk. In the last 12 months, we have seen major attacks on internet-enabled devices and the spread of the so-called "Internet of Things" will see organisations becoming increasingly connected but also increasingly vulnerable. However, lawyers, regulators and other professionals are also developing tools to mitigate cyber risk and organisations have no reason not to be prepared for attacks."

Dino Wilkinson, Partner, Clyde & Co, Middle East

$6trillion

The global cost of cybercrime by 2021

1.8%
The increase in size of data breaches from 2016 to 2017[3]

$170billion
The estimated market size of the cybersecurity industry in 2020[1]

$4mn
The average cost of a data breach in 2016*

$150mn
The average cost of a data breach in 2020*

6000%
Rise in ransomware attacks 2016*

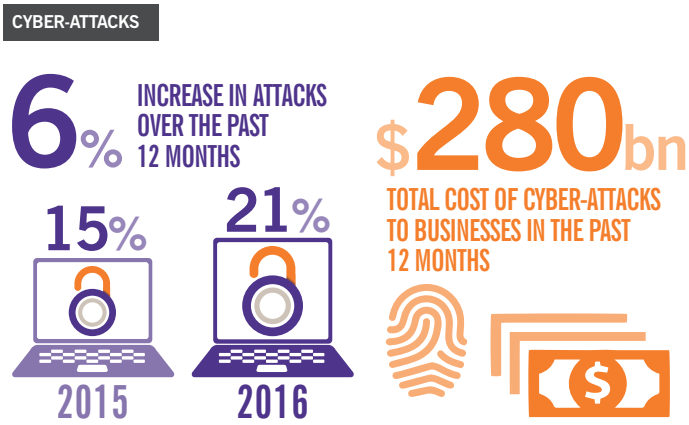
$158bn
Economic losses from natural & man-made disasters in 2016*

Cyber-crime is increasing at a rapid rate which is costing businesses dearly. In just under 12 months there has been a 6% increase in cyber-data crime alone, which has cost businesses $280bn within the same time-period[2].

6000%

rise in ransomware attacks in 2016 which is expected to increase, along with risk.

THE GLOBAL IMPACT OF CYBER CRIME



35%

of organisations are estimated to have cyber-insurance and are protected.

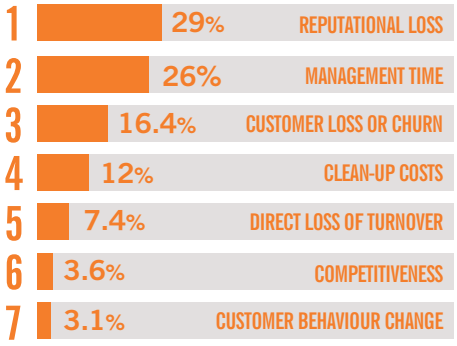
The primary impact of cyber-attacks can have a direct implication on your business, however this is not necessarily quantified by the financial impact alone. Our latest International Business Report found that reputational loss, the amount of management time which attacks consume and the loss of customers were all rated as more prevalent than the direct loss of turnover.

A further sobering statistic was the lack of cyber-insurance which organisations have, with only 35% of organisations protected[2].

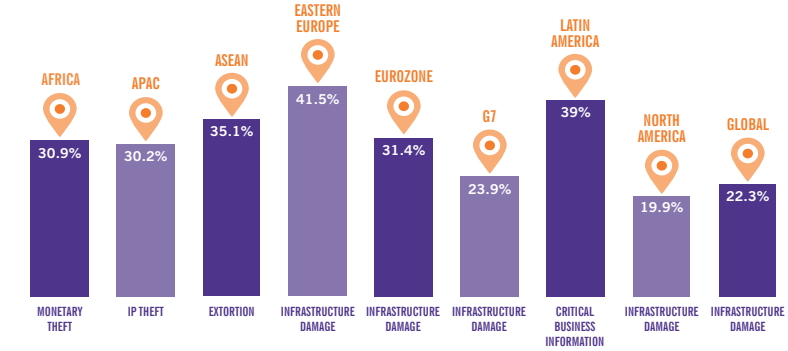
In today's reality, the most common corporate cyber-crime relates to monetary theft, IP crime, data theft and infrastructure damage, which can cost the business millions of dollars to rectify. Our research[2] explored the common cyber-attacks by region, which states that the most frequent destruction to businesses occurred as a result of infrastructure damage.

In a borderless corporate world, it is becoming increasingly important for businesses to educate themselves in respect of the various cyber-threats which they may be exposed to, alongside the relevant regulations which they may need to comply with.

WHAT IS THE PRIMARY IMPACT OF A CYBER-ATTACK?



MOST COMMON CYBER-ATTACKS BY REGION OR COUNTRY GROUPING



While we cannot calculate the global predictability of cyber-crime, we can be assured of its growing prominence which will continue to plague economies and organisations alike for years to come.

All businesses are advised to act now, before it is too late.

To support businesses who have a vested interest outside of their home territory, we explore the top ten countries who have been most affected by cybercrime. The ranking[5] is quantified by the largest sources of malware, spam and phishing attacks.

Country	2016 ranking	2015 ranking	Change	% of threats detected
USA	1	2	▲ Up	23.96%
China	2	1	▼ Down	9.63%
Brazil	3	10	▲ Up	5.84%
India	4	3	▼ Down	5.11%
Germany	5	8	▲ Up	3.35%
Russia	6	11	▲ Up	3.07%
UK	7	7	– No change	2.61%
France	8	8	– No change	2.35%
Japan	9	12	▲ Up	2.25%
Vietnam	10	NA	+ New entry	2.16%

23.96%

the rate of threats detected which has risen from 18.96% for the USA

2.61%

the rate of threats detected remains unchanged for the UK.

Last year the USA, was number two, with 18.89% of threats detected globally, which has now risen to 23.96%.

In 2016, a new kind of malware named Mirai spread around the world, with reports that this originated in the USA. Following closely behind, China was the second-biggest source of global threats detected, down from the number one spot last year. CNBC reported in July that malware originated in China had been found to have infected over 10 million Android phones.

Vietnam was responsible for 2.16% of global threat detections in 2016, up from 0.89% in 2015 as a result of the country being a target of hacking attacks in 2016. In July it was found that Vietnam's biggest airline, Vietnam Airlines had been hacked into, and that malware may have spread to government agencies and banks.

While we cannot calculate the global predictability of cyber-crime, we can be assured of its growing prominence which will continue to plague economies and organisations alike for years to come.

[5] Symantec: 2017 Internet Security Report

Industry viewpoint

Olivier Leblan, Group Chief Information Officer, Chalhoub Group

Technology is evolving at an unprecedented rate and cybercrime follows the same path, becoming a lucrative business, examples have been seen with recent Ransomware attacks.

In the past, cyber threats could be exploited by skilled hackers, now an exploit tool can be purchased as a service and a trending example is ransomware as a service (RaaS) and untraceable (Tor network) Bitcoin transfers.

For family businesses the key focal area will be the internal threat caused by the lack of awareness and training of employees, friends and family members combined with the lack of security governance and investment applied in most businesses.

Do you believe cyber will evolve or be curtailed in the Middle East in the future? Security threats, attack sophistication and complexity is evolving at an alarming pace and we believe it will only be exponential.

No system can be considered 100% secure – we need to make it as hard as possible for the attacker to succeed, and this requires heavy investments in security awareness, processes and tools.

Building our security capability has been at the heart of our strategy for the past 24 months, driven by the rise of Cyber Crime, but also by the rise of customer facing applications and by the nature of data we hold in our systems (more and more customer information). We have therefore started our IT security capability in January 2017 with security at the top of the IT Agenda.

Cyber security is a threat to all businesses, however family business do have a specific context from other types of businesses. Whilst technology is seen as major combatant in most businesses, in family businesses the margin of vulnerability is often greater when it comes to people (family members, friends) and process.

The key strategic aim to protect family run businesses falls on the below considerations:

- Identifying what is most valuable to the organisation and the power that any personal or sensitive information could have if it fell into the wrong hands, ensuring that latest trends are considered, specifically on social media.

- Ensuring that fundamental security controls such as firewalls, anti-virus software, secure configurations, security logging and monitoring are all in place and updated.

- Restricting the use of personal email systems for work purposes. Many family office employees simply use their personal email accounts for correspondence. Not only does this make it harder to manage security, but also opens the potential to security threats.

- Restricting the use of storing sensitive data on external storage devices which have not been encrypted, which would restrict sensitive company data being accessed by hackers or random individuals.

- And lastly with social media playing a large part in our personal and business lives. Agree social media ground-rules with staff and family members. It is impossible to be completely secure however policies and awareness are good tools to combat social media breaches.

Olivier Leblan is the Group Chief Information Officer for Chalhoub Group, one of the largest family owned businesses in the region.

Expert viewpoint:

Cybercrime within owner-managed businesses

George Stoyanov, Transformation Advisory Partner
Grant Thornton, United Arab Emirates

OMBs are undoubtedly a strategic imperative to the global economy, accounting for over two-thirds of all businesses around the world[6], with an estimated contribution of 70-90% of the global GDP annually.

Aside from the financial contribution, these businesses provide an eco-system of talent, given they deliver 50-80% of jobs in a majority of countries worldwide[6].

The scale of OMBs globally, provides further prominence for the need to protect businesses from cyber-attacks. That said, cybersecurity is often given inadequate consideration by OMBs, unless a serious breach has occurred in the past. A recent report by Campden Wealth[7] indicated that 15% of Family Offices surveyed were victims of a cyberattack with losses generally of $50,000 or less, with one incident that cost a family more than $10 million.

Whilst the scale of the loss may seem relatively low in comparison to the global statistic, OMBs have become targets of frequent attacks, given cyber-criminals remain resilient to approach those businesses who choose to pay for a rapid solution rather than investing in building a long-term preventative and protective resolution.

Furthermore, OMBs need to consider the operational, brand and perceptional damage which a cyber-attack can cause particularly given that cyber criminals can often be disguished as disgruntled employees or competitors. There is a need for OMBs to drive behavioural and institutional change, in order to combat this risk.

George Stoyanov,
Transformation Advisory Partner

OMBs, irrespective of size and industry, host several structural challenges which must be addressed in unison with cybersecurity to protect their business from this ever-increasing aggressive crime. These include:

Owner(s) focusing on:

Managing Governance:

Many OMBs who continue to be led by the patriarch operate with flat managerial structures with often limited governance processes, thereby creating daily security alerts across a whole host of elements. That said, institutionalised OMBs may invest in functions which focus on such challenges, however, these businesses remain exposed as a result of their approach to cybersecurity, which is often referred to as a technology matter as opposed to strategic. This mindset exposes businesses to potential vulnerabilities which are not equipped with the adequate resource and infrastructure.

Financial Investment:

As with every business, OMBs focus on growing the business, generating vigorous profits and investing for the future. Such strategic priorities often take precedence in the boardroom which leverages the time and effort of leaders. Technology investment and cybersecurity protection are often placed low on the organisational agenda, thereby exposing the business and its operations further.

[6] Family Firm Institute and European Family Businesses, 2012
[7] Campden Wealth

Directors and family-members focusing on:

Resourcing:

Businesses must address the resourcing challenge which includes access to the cybersecurity workforce, of which there is a global shortage. OMBs are encouraged to rethink the role of the technology position to a cybersecurity and technology development role, whereby the resource is involved with protecting and defending apps, data, devices, infrastructure and people. Lastly, employees need to understand that they are human safeguards, and their training is a critical component of a security plan, therefore security considerations must be given to daily operations, whilst delivering their roles in correlation with the policies and procedures of the business.

In family businesses, the margin of vulnerability is often greater when it comes to people (family members and friends) and process.

Oliver Leblan,
Group CIO, Chalhoub Group

Technology functions:

SME based OMBs often recruit in-house technology support with a remit to managing hard and software, whilst delivering general technological administration, in such cases a conflict of time can often lead to gaps within the infrastructure and ongoing development of crucial platforms. Institutionalised businesses have access to larger and more complex infrastructures, for which qualified resource is essential. These businesses do employ third-party vendors to perform sophisticated vulnerability testing, however financial consideration often deters businesses from ensuring this practice becomes an operational principle.

Infrastructure:

OMBs often suffer from outdated software and hardware alongside limited patch management due to the investment focus of its leaders, which contribute to exposing their business to cyber-attacks. Businesses are encouraged to focus on three core components which will strengthen the organisations infrastructure, these include but are not limited to developing a cybersecurity strategic plan, disaster recovery plan and adequate cyber insurance which will transfer certain risks to a third party.

Ultimately, OMBs must accept that not every cyber-attack can be managed, therefore strategic consideration is required in terms of assessing which risk businesses are prepared to accept, avoid or mitigate, whilst planning for each eventuality by developing a disaster recovery plan.

Managing cyber-risk

Safeguarding owner-managed businesses from cybercrime

Businesses are not immune to cyber-attacks either now or in the future, therefore preventative measures are required to protect employees, owners, customers and the reputation of an organisation. Whilst many businesses have basic network security procedures in place, the level of sophistication being applied by attackers requires a step-change approach, which includes application of the key safeguarding measures below.

1. Treat cyber security as an owner(s)/ management priority

Businesses need to adopt a management approach to cyber-security as opposed to an operational one. The protection of a business should be considered as one of the main strategic priorities for a business, in order to defend its most valuable assets which include data, reputation and confidence. It is becoming increasingly important to develop a cyber and information security governance framework, which will define the cyber strategy, alongside ensuring instantaneous monitoring of both the internal and external threats to the technology environment within the business, through the use of intelligent metrics.

2. Employ a risk based approach

The first step to preventing cyber-attacks is to assess the exact risks: determine key assets and processes, pinpoint vulnerabilities, determine the most pressing threats which may affect the bottom line and identify areas of improvement. The risk assessment should focus not only on the current state of the business but also consider its growth strategy, and the technological needs going forward.

3. Create a robust cyber-security policy

The risk assessment results should be integrated into a robust, cyber security policy which focuses on people, processes and technology. A centralised policy will form as a set of principles which the business can apply in a uniformed manner, whilst providing enough flexibility for functions and departments to adjust according to their workflow or business needs, without comprising the bottom line or security of the wider business. The plan should be a live document which evolves with the organisation and cyber trends, whilst identifying the most important systems and data as well as appropriate protections and access controls.

4. Ensure response and incident procedures are in place to manage a crisis

It is important that businesses react quickly in case of a cyber incident, and follow a strict protocol in controlling damage both internally and externally. Cyber security policies should include a clear outline of measures and of resources available in case of an incident, which should include communication protocols for reputation damage limitation purposes.

5. Comply with industry leading practices

Businesses should work towards obtaining relevant accreditation of its information and cyber security practices, certificates such as ISO 27001 or COBIT will support the business with its compliance levels, whilst meeting the relevant prevention and protection requirements. Such endorsement can also often act as a deterrent for attackers, who will often be phased by the level of security available within the business.

6. Adopt safety measures

Businesses can adopt several safety measures which will go some way to protecting data, assets and closing any gaps which may exist, some of these measures include:

• Applying strict criteria to vendor selection

• Securing websites against attacks and malware infections, alongside regularly monitoring potential vulnerabilities

• Adopting encryption principles to protect sensitive data

• Restricting email attachments and consider blocking commonly used attachments which spread viruses

• Enforcing effective password policies for multiple platforms, with regular changes encouraged

• Aggressively updating, patching and migrating from outdated browsers, applications and plug-ins and;

• Performing annual vulnerability assessment and penetration testing.

7. Back up data

Data backup is a basic security measurement which businesses often neglect and which is becoming increasingly relevant as attacks surge. Data backup should be thoroughly protected and encrypted, with cloud being considered where possible and feasible, along with ensuring the responsibility of data backup is appropriately allocated to several employees, in order to avoid internal security threats.

8. Protect smartphones and handheld devices

If your business network is open for the personal use of employees and visitors, then it is important to ensure a minimum level of security profile is in place. It is advisable that smartphones and handheld devices are treated as mini-computers and protected accordingly, this includes having biometric access control, automated device back up, regular updates and restricting the use of jailbreak devices.

9. Invest in cyber-insurance

Aligning with the risk assessment, businesses should consider purchasing cyber insurance in order to transfer certain risks to third parties. It is worth being aware that underwriting cloud infrastructure may be different from underwriting on premise systems, therefore policies should be reviewed in detail and in alignment with your cyber strategy.

10. Educate employees

Building a cyber-secure culture is perhaps the broadest area of development for businesses. From social media policies to cyber security training, businesses need to create awareness and foster the right behaviours amongst their people. Businesses can proactively create awareness amongst its employees, particularly around the prevalence of phishing scams which occur as a result of clicking on embedded links which redirect the user to a suspicious URL or website which may appear legitimate. Likewise, it is essential to educate all employees across each grade, of the importance of withholding personal or professional information of any kind, irrespective of the sender's name which can often be disguised as an internal colleague of the business.

Checklist:

Safeguarding your business

- ☐ Treat cyber security as an owners/ management priority
- ☐ Employ a risk based approach
- ☐ Create a robust cyber-security policy
- ☐ Ensure response and incident procedures are in place to manage a crisis
- ☐ Comply with industry leading practices
- ☐ Adopt safety measures
- ☐ Back up data
- ☐ Protect smartphones and handheld devices
- ☐ Invest in cyber-insurance
- ☐ Educate employees

Contact us

We help our clients prepare themselves for cybersecurity threats, ensure ongoing protection, react effectively to attacks and drive change to improve their cybersecurity capability.

To explore how your business could improve information management and minimise cyber risk, please contact us.

George Stoyanov
Partner
E george.stoyanov@ae.gt.com

Dubai
Rolex Tower,
23rd floor,
Sheikh Zayed Road,
Dubai, UAE
T +971 4 388 9925
F +971 4 388 9915

Abu Dhabi
Office 1101, 11th floor,
Al Kamala Tower,
Zayed the 1st street, Khalidiya,
Abu Dhabi, UAE
T +971 2 666 9750
F +971 2 666 9816

E: grantthornton@ae.gt.com
W: www.grantthornton.ae

About Grant Thornton
Grant Thornton is one of the world's leading organisations of independent assurance, tax and advisory firms. These firms help dynamic organisations unlock their potential for growth by providing meaningful, forward looking advice.

Proactive teams, led by approachable partners, use insights, experience and instinct to understand complex issues for privately owned, publicly listed and public sector clients and help them to find solutions. More than 47,000 Grant Thornton people across over 130 countries, are focused on making a difference to the clients, colleagues and the communities in which we live and work.

To read more about cyber resilience or how we can help, visit grantthornton.ae

Grant Thornton
An instinct for growth™