Grant Thornton
An instinct for growth™

How to be cyber-secure?

Act now, before it's too late

The Grant Thornton International Business Report (IBR)*, a global survey of 2,500 business leaders in 35 economies, has revealed that over the past 12 months more than 15% of businesses across the world have suffered a cyber-attack, costing a total of more than $300 billion. That's just the measurable costs. Who knows what the reputational damage, loss of trust and custom adds up to.

52%
OF GLOBAL BUSINESSES HAVE A CYBER-SECURITY POLICY IN PLACE NOW

Many of the perpetrators of cyber-attacks are sophisticated, heavily resourced criminal organisations. They can strike without warning and sometimes without the victim being immediately aware that they are under attack.

But it's not just the cyber criminals that organisations need to worry about. As more and more high-profile hacks make headlines, customers are increasingly aware of their vulnerability online. Client/customer demand for better online protection is the number one factor that is driving businesses to implement cyber-security strategies. And if those strategies fail, customers will simply go elsewhere.

Unfortunately, just 52% of businesses globally currently have a cyber-security policy in place. This, in our view, is still too small a percentage.

In this paper, based on the insights from Grant Thornton cyber specialists from around the world, we explore the motivations and tactics of cyber-attackers. We also consider what organisations need to do to put effective defences in place around the three pillars of people, process and technology.

Vigilance alone won't keep organisations safe; proactive measures are needed. This is an issue that needs to dominate the agenda of boardrooms, IT departments and all staff, before it's too late.

Paul Jacobs
Global leader – cyber security

* *All figures are based on data from the 2015 Grant Thornton International Business Report*

Cyber-attackers: identities, motives and tactics

Type 'cyber-crime' into any search engine and you'll get an array of pictures of shady-looking young men in hoodies, hunched over laptops in dark corners. Today, that stereotype couldn't be further from the truth.

Cyber-attackers, who once acted in isolation, have evolved into organised, skillful, extremely agile profit-driven businesses that usually operate internationally to make it harder for national crime agencies to track them down. Increasingly, they use underground supply chains to develop, distribute and deploy customised malware to carry out attacks. New Grant Thornton research suggests the direct impact of cyber-crime is now costing companies more than $300 billion a year globally.

Mike Harris,
Grant Thornton Ireland

"There is a very, very sophisticated cyber-crime supply chain in existence in the world. It is commercially driven and highly outsourced."

Motivations for cyber-crime

Financial gain is the main motive behind cyber-crime, but hackers are also launching attacks for a number of other reasons.

Extra-marital affair website Ashley Madison was recently targeted by 'hacktivists' who disclosed clients' personal data, claiming their actions were driven by a moral imperative. In 2013 hacking group Anonymous attacked the websites of PayPal, Visa and Mastercard for failing to process donations to Wikileaks.

A number of governments have been accused of sponsoring attacks that target corporate intellectual property (IP) and industrial secrets as they seek to gain a competitive advantage in a globalised economy. IP-motivated attacks are executed at an organisational level too. Manufacturer Dyson has had its intellectual property stolen without any apparent action against the perpetrators taken by official authorities in the country where the theft took place.

Yet, state-sponsored attacks aren't always IP-related. Professional hackers will attack a company's technology to demonstrate its weakness, and therefore untrustworthiness, to the world. In July 2015 Fiat Chrysler was forced to recall 1.4 million vehicles after hackers highlighted a software security flaw that allowed the engine to be turned off remotely.

Some companies fall victim to criminal or terrorist organisations that are trying to launder stolen funds, while other attackers are simply on a 'fishing' expedition to see if anything of value or interest is out there. And, despite the outdated image of young men in 'hoodies' hunched over laptops, bored tech-savvy teenagers in bedrooms around the world still deface websites or hack into an unsuspecting victim's personal account just to be annoying or malicious.

Typical motivations

Financial gain Moral crusade **Theft of intellectual property** Money laundering **Highlighting technology flaws** Restricting access **Boredom**

How hackers attack

How hackers attack varies, but as incidents occur more frequently, hack-watchers are starting to identify patterns between motives, tactics and the location of the origin of the attack.

Hacks originating from Russia, for example, tend to be targeted and in search of personal financial information that can quickly be sold on for financial gain. Attacks originating from China, or associated countries, tend to target proprietary IP held by a range of organisations, such as educational institutions, health sciences companies and technology firms.

Kevin Morgan,
Grant Thornton US

"Foreign hackers have a habit of being very specific and targeted. When they identify a target, they'll plan and execute an attack against them very quickly. Countries that have a larger volume of hackers continuously scan many types of firms that they believe might have valuable IP, and when they find something that has potential value, they easily exploit it."

Savvy attackers will use technology to mask their location, or even steal the identity of a local user – an employee within the targeted organisation with super-user rights, for example – to launch an attack. The onus then falls on the victim to prove their identity was hacked.

Phishing – the use of fake sites masquerading as the real thing – is a popular and long-used tactic for gaining the personal and financial details of unsuspecting customers. New Zealand's Inland Revenue Department (IRD) fell victim to this last year when scammers used a fake IRD-branded website, offering speedy tax refunds to gain the bank account details of thousands of citizens.

Distributed Denial of Service (DDoS) attacks are growing in frequency – such as those executed by Anonymous on payments companies, flooding websites with online requests to the extent that they could no longer operate effectively. Attackers often use DDoS attacks to demand ransoms of around €5,000 to €10,000 – a small enough amount to collect quickly – before moving on to the next victim.

In a more insidious approach, hackers recently launched a low level DDoS attack on UK-based telecoms company TalkTalk as a distraction tactic. In parallel they ran a more serious 'SQLi' attack to breach the company's networks and steal the bank account and personal details of at least 400,000 customers.

Skip Westfall,
Grant Thornton US

"DDoS is a very powerful tool, not just from a hacktivist's point of view but from a high-value ransom point of view against organisations who bleed money if they're not operating 24/7."

Many companies don't even know they've been hacked until they hear about it from a third party. These so-called 'indirect hacks' are expected to increase.

Manish Chawda,
Grant Thornton
Singapore

"There are going to be many more cyber-attacks, but most organisations will actually never know they've been compromised until it's too late, or in most cases months or years will pass before discovering the compromise."

Cyber-attacks are on the rise

More than one in six businesses surveyed (15%) for the Grant Thornton IBR research faced a cyber-attack in the past 12 months. Businesses in the European Union (19%) and North America (18%) were the most heavily targeted.

This could be just the tip of the iceberg. As more and more potential attackers realise the financial benefits that can be gained, we can expect the number of attacks to increase. Mid-sized organisations will be just as vulnerable, as large corporates and attackers will expand their reach to all four corners of the globe.

Paul Jacobs,
Grant Thornton Ireland

"The analogy is with the iceberg. We're actually only seeing a small percentage above the waterline. We would certainly expect to see the number of cyber-attacks grow in the foreseeable future because, quite clearly, there's a financial benefit to be gained and cyber-criminals continually innovate to exploit weaknesses in control environments, IT systems and our people."

Countries which may not have traditionally considered themselves to be in the firing line, will increasingly be targeted. In March, security vendor Trend Micro identified Australia and New Zealand as twice as susceptible to CryptoWall 3.0 as the rest of the world. The CryptoWall ransomware is designed to steal and hold valuable data from infected systems until a Bitcoin ransom is paid.

Hamish Bowen,
Grant Thornton
New Zealand

"As a country, New Zealand has been pretty naïve about cyber-security. Because of our physical isolation, we've always been a fairly trusting people; there is a cultural element that supports a poor attitude towards security. Only now are executives and boards waking up to the risks posed by cyber-security."

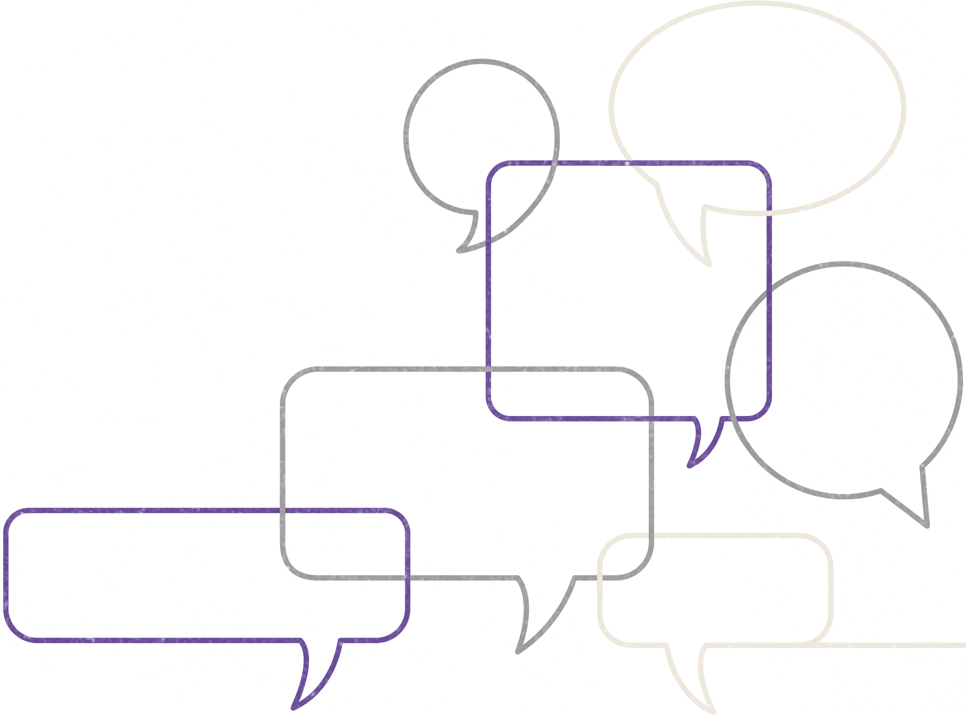
The increasing prevalence of technology in our professional and personal lives will increase the chances of cyber-crime occurring. The Internet of Things, in particular, which will connect our communications devices, our cars and our homes together, will present hackers with new avenues of attack. But old avenues shouldn't be forgotten. Legacy technology systems, which are more likely to be unprotected, will continue to be exploited too.

Michiel Jonker,
Grant Thornton
South Africa

"We are living in a volatile, uncertain, complex and ambiguous world. The continuous integration of systems, business borders and country borders is increasing this complexity. There are more than three billion people already on the internet and this is going to increase exponentially. We will have to focus more on resilient strategies and controls in the future to deal with cyber-crime. I foresee a move to resilient controls rather than robust controls. Robust controls are preventative controls but these are failing. We will have to have a paradigm shift in our thinking towards robust controls, which focus on detection and how quickly you can contain an incident."

Matthew Green,
Grant Thornton
Australia

"There's a global concept called 'privacy by design', which is all about designing in privacy controls when building new systems and processes. You could argue that 'security by design' or a similar concept is very much required now to prepare for this ongoing convergence."



How vulnerable are you?

Companies are more vulnerable to cyber-attacks than they might think, particularly those with large digital footprints. Demand for cyber-security services and recognition of the importance of cyber-security controls has come, for the most part, from the financial services industry. However, other sectors that are increasingly technology driven – retail, manufacturing and media, for example – are now taking note.

Cyber-criminals are constantly looking for weaknesses in a company's defences, such as an absence of mechanisms to monitor the robustness of an organisation's IT infrastructure – the equivalent of having no security guards on your perimeter, if you like. And the majority of companies are still poor at monitoring. Recent research in New Zealand revealed that the average period between a cyber-attack occurring and it being discovered was a staggering 300 days. Companies also seem to struggle with simple measures such as updating their systems with security patches that software providers release on a fairly regular basis.

Michiel Jonker,
Grant Thornton
South Africa

"The majority of companies don't know what is going on in their IT network. They would not be able to tell you of any suspicious activity or sense that activity through context-aware systems. They are unable to tell you if there are fraudulent transactions occurring because of a firewall breach. A resilient approach is not there. That is one of the weaknesses that I see in South African companies."

Companies become even more susceptible to attacks as their digital footprint grows to envelop their supply chains, including outsourcing providers.

US retailer Target's high-profile data breach in 2014, which led to the theft of the personal contact details of 70 million customers and the credit card details of 40 million shoppers, occurred after hackers stole login details to the company's network from a facilities supplier. The hackers made $53.7 million from the attack, which resulted in the resignations of Target's CEO and CTO.

Home Depot, another US retailer, suffered an eerily similar attack in the same year. Hackers stole 56 million customer credit and debit card accounts and made off with 53 million customer email addresses after gaining access to the company's network via a third-party vendor. The attack cost Home Depot an estimated $62 million, and an additional $90 million to replace the stolen credit and debit cards.

Rikki Sorensen,
Raymond Chabot
Grant Thornton Canada

"As more organisations go to market online and interact with their partners in a state of trusted connectivity – where data or systems are shared, for example – the attack surface for hackers will continually increase. Most large organisations are capable of securing their network. But, as more and more of them increase their use of outsourced yet connected services and third party technologies, the challenges around preventing and detecting cyber-attacks and breached also increase."

Kevin Morgan,
Grant Thornton US

"Third party risk, particularly with the amount of outsourcing and out-tasking that now exists, is clearly a high risk vector in the US; particularly with the pressure to reduce expenditures by bringing in more cost effective suppliers. It is critical to continuously assess your vendors' management processes to ensure they are protecting your organisation's data with the same seriousness you are."

In the wake of an attack, the first instinct may be to focus cyber-security efforts on technology systems, but it's often an unsuspecting employee who accidentally opens the door to let hackers in. In fact, lack of user education is one the biggest factors driving cyber-attacks in mid-market companies, which often use similar IT networks to large corporates but lack the resources to train staff on how to be cyber-secure.

Hamish Bowen,
Grant Thornton
New Zealand

"Companies tend to see security as a technology problem but if you're going to be compromised, technology can only protect you to a certain extent. What you usually find is that someone has clicked on the wrong thing or inadvertently disclosed the wrong information and let the attacker in. There's nothing you can do from a technical perspective to overcome people who are the weakest link."

In some instances, however, strong monitoring mechanisms and a vigilant workforce still won't be enough to deter cyber-attackers. To understand their degree of exposure to cyber-risk, companies need to ask themselves whether they have anything worth stealing.

Manish Chawda,
Grant Thornton
Singapore

"You would assume that high profile organisations like NASA and the US National Security Agency have enough controls in place to stop hackers. Unfortunately, they've all been hacked along with a number of other governments that have appropriate controls in place. Hacking is not based upon the weakness of a company; it's based upon the value of the assets that a company owns and the worth of that asset to the cyber-criminal. Do you have something worth stealing?"

Why companies are failing to act

Despite these risks and vulnerabilities, our research found that a surprising 48% of firms are putting themselves in the firing line, with no comprehensive strategy in place to prevent cyber-crime. Many organisations believe they have "nothing worth stealing", while the mid-market response is often to plead a lack of resources. But a shortfall in experience and awareness of the importance of cyber-security at board and senior management level is the main reason why it goes unaddressed.

Mike Harris,
Grant Thornton Ireland

"We have a challenge in Ireland, specifically around the level of non-executive director knowledge of cyber-security. Board members who, for example, come from the UK would have a much higher level of knowledge because I think there's a more structured approach from the UK government around educating non-executive directors."

The UK government has written to the chairmen and audit committee heads of companies across the country, requesting details about their cyber-risk management policies. It is, more than anything, an attempt to ensure companies are addressing the isssue.

Ali Jaffer,
Grant Thornton Canada

"I think most organisations have seen others put a policy in place and for it to have no or little effect on improving the cyber-security posture of that entity. So there is an inherent perception that many policies, once implemented, don't necessarily have the desired effect or outcome. I think that's part of the reason why you see a lack of attention to putting such mechanisms in place."

In this tough economic climate, other priorities can also take over. The South African Institute of Risk Management puts cyber-crime at number six in its list of the top ten risks facing South African companies by likelihood, but cyber-security should be in every organisation's top five, if not top three, risks. Unfortunately, too many organisations don't appreciate this and are ill-prepared. Many fail to include cyber-risk in their enterprise risk management programmes; something that should be done as a matter of best practice.

In Canada, the federal government is leading by example. Shared Services Canada, which owns and operates the entire government's IT infrastructure, ranks cyber-security as its number one risk.

Manu Sharma,
Grant Thornton UK

"Cyber-security is a high risk but I think the way to look at it is from an impact and consequences perspective rather than directly from a risk perspective. What impact would a cyber-attack have? Have we done a proper assessment to identify what it could lead to? Cyber-security should be a priority if it's a threat to resilience."

How organisations can protect their assets

Organisations cannot expect to be completely insulated from cyber attacks but it's essential to have a cyber-security policy in place that is continuously evaluated for its effectiveness.

Manish Chawda,
Grant Thornton
Singapore

"There is a small, highly skilled core group of hackers, perhaps 0.01% of the total experienced, skilled hackers who can come compromise an organisation, steal or add malware, get in and out without the organisations ever realising. No organisation is 100% secure, but by implementing the appropriate detective and preventative controls, you can deter or stop the other 99.99%."

There is no 'one-size-fits-all' approach to cyber-security, but the strategies that work are built around three pillars: people, processes and technology. Organisations that get this right educate their people to be their first line of defence, building a culture of security awareness; they implement the right security processes; and they use technology to enforce those processes, where necessary.

What does that mean in practice? Cyber-security strategies should be tailored to fit an organisation both operationally and culturally, taking account of regulatory demands within the given jurisdiction and focusing on what needs to be protected most rather than offering blanket coverage.

Rikki Sorensen,
Raymond Chabot
Grant Thornton Canada

"So many organisations draft a cyber-security policy based on a particular standard or something published online, but at the end of the day most don't fit the organisation or drive the right behaviours and achieve the right results. So, as soon as an organisation gets to the point where the policy is recognised as being ineffective or unachievable, the motivation behind it completely drops and it becomes a useless tool."

Hamish Bowen,
Grant Thornton
New Zealand

"If you're continually trying to secure everything, you're wasting your time and energy. Most cyber-security programmes I see often fail because they start with good intentions but then they try and boil the ocean; they focus on stuff that really isn't perceived as relevant."

Identifying priorities for protection starts with a risk assessment and gap analysis. Continual reassessment is important to ensure that the right areas of an organisation are always protected. Performance of the strategy needs to be consistently monitored for effectiveness too.

Kevin Morgan,
Grant Thornton US

"If you don't have the resources, processes or capabilities to monitor or understand the performance of your organisation against a particular policy or a set of expectations, then it's really going to be for nought at the end of the day. An organisation must remain vigilant and proactive to protect itself from an attack."

The board, the CEO and business unit heads need to take overall responsibility for the success of the strategy, rather than leaving it to the IT department. In some parts of the world company boards are starting to wake up to the importance of cyber-security as high-profile data breaches make headlines and regulatory authorities demand better governance on the issue. In the US, for example, where audit committees have traditionally been tasked with ensuring compliance with cyber-security policies, anecdotal evidence of boards recruiting for members with cyber-security expertise suggests directors are preparing to take a more hands-on approach.

That said, everyone across the organisation should be aware of and understand the role that they have to play in making their firm cyber-secure.

Rikki Sorensen,
Raymond Chabot
Grant Thornton Canada

"No doubt, it has to start from the top, but the responsibility for cyber-security should lie with every single individual in the organisation. The challenge is to make any policy, guidance or training relevant to the common employee and build a culture of awareness, not just compliance to training and awareness. Getting the collective culture of an organisation to understand how their daily actions such as clicking on an unknown link in an email can cause serious harm to the organisation is the real goal here."

Firm-wide accountability is achieved by cascading agreed policies down to all employees through awareness-raising and training programmes that help to make the cyber-threat relevant to each and every individual. This top-down communication should always be genuine; not a tick-box exercise.

Effective policies and strategies embed cyber-security within the success metrics of an organisation. That contributes towards a culture in which everyone takes the issue seriously at all times and shares ownership.

Skip Westfall,
Grant Thornton US

"You want an entire culture that is aware and on top of security. When the stakeholders of business units are able to marry cyber-security with their success metrics in a way that doesn't, in their minds, block them from getting where they need to be, that's when you're really changing the culture of the company."

At that point, when cyber-security is not seen as a one-off project but as part of the DNA of an organisation, entities might be able to rest a little easier about the circling cyber-threats.

Hamish Bowen,
Grant Thornton
New Zealand

"Cyber-security has got to be something that's business as usual. You've got to set it up to be something that you're constantly managing, enhancing and working on."

Creating effective cyber-security policies: pitfalls to watch for

Lack of board and senior management buy-in

Policies that lack robustness, breadth and depth – Effective policies should outline procedures, mechanisms and controls for implementation; communication procedures; and monitoring processes

Failure to update training, policies and procedures to reflect the changing nature of cyber-threats

Failure to align people, processes and technology

Lack of internal skills and capabilities to implement cyber-security policies effectively

Writing overly technical policies that fail to connect with employees

What are governments doing to help?

Governments' response to cyber-crime has, on the whole, been slow and inadequate. Many Asian countries still don't require mandatory reporting of data breaches, which could be why companies in the region are targeted around a third more than the global average – a figure reported by US security network company FireEye Inc.

New Zealand is another country that doesn't compel its companies to report cyber-attacks, although that may change as the government seeks to gain a greater slice of global trade. In 2011 its government published a cyber security strategy that outlined three priorities: increasing awareness and online security; protecting government systems and information; and incident response and planning. The strategy also led to the launch of the National Cyber Security Centre.

In Ireland, the repercussions for cyber-criminals are limited. The local courts have convicted less than ten people, with sentences totaling less than ten years behind bars.

Ali Jaffer,
Grant Thornton Canada

"If we wait for governments to implement policies and standards, it's going to be a long time before we see them implemented and having an effect. The need for change really is today."

However, other countries are getting their act together. Launched in 2014, the UK's National Cyber Security Programme sets out five technical controls that will protect firms against the majority of cyber-threats. Several household names have already gained Cyber Essentials accreditation by adopting these controls, including Vodafone, Barclays and GlaxoSmithKline.

The US continues to indict and move forward with the extradition of perpetrators of cyber-crime – the FBI is working proactively around the world to identify cyber-criminals and track them down.

Singapore's government is putting regulations in place to ensure that the city-state becomes a safer place in which to do business, while South Africa recently passed a Protection of Personal Information Act. Clauses dealing with the set-up of an Office of the Regulator are already in effect; remaining clauses will come into force once the regulator is fully functioning, which is expected to happen in 2017. The Cybercrimes and Cybersecurity Bill is also going through the South African parliament.

The Australian government set up the Australian Cyber Security Centre in November 2014 and data breach notification legislation is on the horizon. However, much more can be done.

Matthew Green,
Grant Thornton Australia

"Law enforcement [in Australia] is probably under-prepared to deal with cyber-security issues so there's perhaps a need for greater investment in that area. Second only to Europe, Australia has some very strong data privacy legislation. That's a great building block that needs to be enhanced through things such as mandatory data breach notification and stronger supporting guidance for compliance."

Clearly, governments and regulators need to play a much bigger part in identifying cyber-attacks as an organisational risk, as well as educating their people of the dangers. Government agencies need to improve their collaboration with each other, while rules across different jurisdictions need to be harmonised. That said, governments and regulators don't have the resources or skills needed to fight cyber-criminals on their own – the private sector needs to play its part too.

That doesn't necessarily need to be on a company-by-company basis. In countries such as Canada and New Zealand, financial services entities are pulling together to fight cyber-crime as an industry. The sector is almost definitely the leader in taking this approach.

Ali Jaffer,
Grant Thornton Canada

"Payment card companies have been criticised time and time again, with a lot of hacks and mismanagement from so many different organisations on how credit card information was handled, so they came together and built a set of industry standards. It has been industry driven and I think that's the best approach – organisations coming together to collaborate and define expectations, share knowledge, share experiences and really drive better practices."

Mike Harris,
Grant Thornton Ireland

"Consumers need to be more aware of cyber-security risks as well. You don't go into a swimming pool unless you can swim. In the same vein, you shouldn't be buying things on the internet unless you know about cyber-crime and you know how to protect yourself a little bit."

The consequences of failing to act

Failing to shore up your cyber-defences can be costly and, at worst, threaten the very survival of a company. The direct financial hit that an organisation takes doesn't account for the long-term reputational damage and loss of trust that it suffers when its systems are breached. Operational damage can last for months; when US entertainment giant Sony was hacked in 2014 it couldn't deliver audited financial statements at the beginning of 2015 because its systems were still down.

Paul Jacobs,
Grant Thornton Ireland

"Rebuilding IT systems can be time consuming and expensive. Management and staff time spent on dealing with the fallout of a cyber-attack can often outweigh the direct cost of the attack itself, while regulatory fines can be an additional expense. Longer term, the theft of intellectual property can permanently damage a company's competitive advantage and shift custom to rivals. And as customers start to lose trust in online interactions, companies' digital strategies could be affected."

Lloyds of London insurer Aegis London, which underwrites cyber-insurance for a global client base, says attacks are becoming increasingly destructive and fully expects an organisation to fail in 2015 due to the financial consequences of a cyber-attack. Research by global reinsurer PartnerRe and Advisen, an insurance intelligence firm, found that between 2006 and 2013 there was a five-fold increase in cyber-insurance purchases. Current estimates suggest the global cyber-insurance market is worth more than $1 billion.

Mike Harris,
Grant Thornton Ireland

"A cyber-attack can be catastrophic from a financial perspective and in some cases it can be an existential risk to an organisation. We had a data breach in Ireland of a company that ran loyalty programmes for a large number of multinationals. They had a major credit card hack, which effectively put the organisation out of action for six months and they barely survived it."

Kevin Morgan,
Grant Thornton US

"Home Depot, Target, Ashley Madison – these organisations have been decimated and have lost millions of dollars from cyber-incidents. Cybersecurity isn't just the CIO's responsibility anymore, it is a shared responsibility throughout the executive level of an organisation."

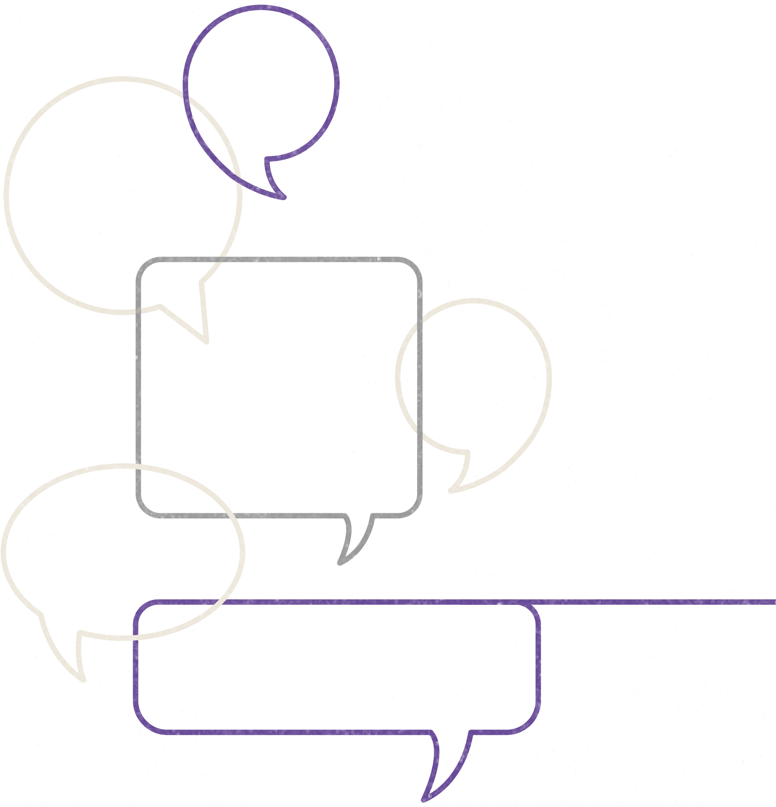
As serious as financial loss and company collapse is, when government agencies are hacked the consequences can be much graver. In 2011 the Canadian federal government suffered a major attack which resulted in breaches of highly classified government and military information.

Rikki Sorensen,
Raymond Chabot
Grant Thornton Canada

"Past and present cyber-attacks against the Canadian government, like the more successful and widely published breaches of 2011 and 2015, degrade the political and business trust that other nations and trading partners have in our federal government institutions and in Canada as a whole. Ultimately, these type of events can publicly call into question any organisations' ability to effectively secure sensitive or privileged information. These types of attacks can do irreparable and long-term damage to organisations and can quickly erode diplomatic relations between nations. Unfortunately, there's no easy or quick fix. Loss of trust has a real dollar cost associated with it, both operationally and in economically strategic negotiations. In most cases, the time needed to rebuild trust or a key relationship, delays or destroys key economical and trading opportunities for both the government and private industry."

When Edward Snowden leaked 1.7 million classified files from the US National Security Agency in 2013, the US government said his actions had put the lives of its intelligence agents and their contacts at risk.

Whatever the consequences, failing to act would be a grave dereliction of a company's duty of care to its stakeholders, from customers, employees and suppliers to investors and society at large.



Defence is the best form of attack

Cyber-criminals are growing in number and defy stereotypes. Victims can never know if their predator is a nation state, a corporate competitor, a criminal gang or a bored teenager. Increasingly complex and interconnected technology systems make it easier for attackers to hide. They could be on the other side of the world or in our midst. Most of the time, we just don't know.

When your enemy is elusive, defence is the best form of attack. A watertight cyber-security strategy is only the starting point. Senior executives need to lead their organisations from the front, extolling the importance of cyber-security and genuinely believing in what they say. Employees need to play their part too, making cyber-secure behaviour a daily part of their working lives. And the wider corporate world needs to start valuing cyber-security as an indicator of organisational success.

These measures may not stop the 00.01% of determined or most skilled hackers who have your valuable assets in their sights, but they will stop the 99.99% of attackers who are currently pushing at an open door.

About Grant Thornton

Grant Thornton's specialists work with clients across the globe to help them understand and respond to cyber-security threats to their organisation. The team assesses risk and helps improve culture, technologies and processes to manage that risk. In addition, our specialists help organisations identify, respond to and investigate cyber-security incidents and breaches.

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 40,000 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.

For more information about Grant Thornton, visit www.grantthornton.global

Contact our specialists

Paul Jacobs
Global leader
of cyber security
Grant Thornton Ireland
+ 353 (0)1 680 5835
paul.jacobs@ie.gt.com

Matthew Green
Grant Thornton Australia
+61 3 8663 6168
matthew.green@au.gt.com

Ali Jaffer
Grant Thornton Canada
+1 416 607 2612
ali.jaffer@ca.gt.com

Rikki Sorensen
Raymond Chabot
Grant Thornton- Canada
+1 613 760 3523
sorensen.rikki@rcgt.com

Mike Harris
Grant Thornton Ireland
+ 353 (0)1 436 6503
mike.harris@ie.gt.com

Hamish Bowen
Grant Thornton New Zealand
+64 (0)27 489 9997
hamish.bowen@nz.gt.com

Manish Chawda
Grant Thornton Singapore
+65 6805 4121
manish.chawda@sg.gt.com

Michiel Jonker
Grant Thornton South Africa
+27 10 590 7240
michiel.jonker@za.gt.com

Manu Sharma
Grant Thornton UK
+44 (0)20 7865 2406
manu.sharma@uk.gt.com

Kevin Morgan
Grant Thornton US
+1 203 3278295
kevin.h.morgan@us.gt.com

Skip Westfall
Grant Thornton US
+1 832 476 5000
skip.westfall@us.gt.com

Grant Thornton
An instinct for growth™

'Grant Thornton' refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires.

Grant Thornton International Ltd (GTIL) and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.

www.grantthornton.global

Curious Agency 1511-05