Grant Thornton

An instinct for growth™

How safe is your organisation?

Take steps now to defend against cyber-attacks

A fresh perspective that helps you stay one step ahead

True success comes from working with a partner you trust to provide the insight, support and expertise that will propel your business forward. Working with Grant Thornton means you can count on results, partnership and leadership.

42,000 people and growing

730 offices and growing

presence in 133 countries

At Grant Thornton, we spend time understanding your needs. This combined with our security expertise, industry knowledge and proven methodology will help you understand, prioritise and address any security issues you may have. We have performed assessments for multinational clients, financial institutions, and government organisations among others. This has given us deep experience with the Maltese and European regulatory requirements along with business and practical experience across a broad range of industry sectors.

Grant Thornton is a US$4.5 billion global organisation with more than 42,000 people in over 130 countries. That's a lot of resources and a broad range of services but we're still small enough to deliver a highly personalised service. It's a best of both worlds approach where we can recognise our clients' needs whilst drawing on our deep global expertise. This means that we make use of proven security assessment methodologies, frameworks and techniques that have proven to drive actionable results for our clients across the globe.

Founded in 1975, the Malta firm became a Grant Thornton member firm in 1991. We have been building our momentum for over 40 years, garnering hands-on experience thanks to the trust placed in us by our clients, offering a range of services that promise to stand the test of time.

Understand the threat: prevention is better than cure

It's becoming increasingly difficult to detect cyber attacks and resolve the security issues created by them. According to a research conducted by the Ponemon Institute: the average time to detect a malicious or criminal attack by a global study sample of organisations was 170 days, with 68% of the funds lost as a result of a cyber attack being declared unrecoverable.

The Grant Thornton 2015 International Business Report, a global survey of 2,500 business leaders in 35 economies, has revealed that in 2015 more than 15% of businesses across the world have suffered a cyber-attack, costing a total of more than €300 billion, whilst some vendor and media forecasts over the past year put the cybercrime figure as high as $500 billion and more.

From 2013 to 2015 the cyber crime costs quadrupled, and it looks like there will be another quadrupling from 2015 to 2019. Juniper research recently predicted that the rapid digitisation of consumers' lives and enterprise records will increase the cost of data breaches to $2.1 trillion globally by 2019, increasing to almost four times the estimated cost of breaches in 2015. That's just the measurable cost. Who knows what the reputational damage, loss of trust and custom adds up to.

The World Economic Forum (WEF) says a significant portion of cybercrime goes undetected, particularly industrial espionage where access to confidential documents and data is difficult to spot. Those crimes would arguably move the needle on the cyber crime numbers much higher.

Data is increasingly playing an important part in the global economic landscape. As we seek to provide more efficient services or gain more meaningful insights into consumer behaviour, we are collecting and storing more and more information. This information has become a valuable commodity to many and as such the collection and use of this data is a growing area for the international community in terms of legislation and enforcement.

How do they threaten your business?

No industry is safe: all business sectors are affected to a higher or lower degree. Cybercriminals hunt for soft and lucrative targets to attack. In the healthcare industry, the street value of stolen medical information is $50 per record, compared to $1 for a stolen Social Security number (source: The World Privacy Forum 2015). Breaches in the healthcare sector topped the Identity Theft Resource Center 2014 Breach List, with 43% of the incidents identified in 2014. The fresher the data, the higher the value on the black market.

The financial services sector is a frequent victim, with 39% of the financial companies surveyed by a big four firm reported being hit by cybercrime. That compares to 17% in other industries.

Other verticals targeted frequently by cybercriminals include education and government. Retailers also provide a perennial target for cybercrime groups. Several of the hacked large retailers spend hundreds of millions of dollars replacing credit cards and paying for credit monitoring services for their customers.

68%
of funds lost through cyber attacks are declared unrecoverable?

cyber crime costs projected to reach
$2 trillion
by 2019

Among all cyber crimes, insider threats are the most expensive to deal with.

59%
of employees steal corporate data when they quit or are fired.

Have you already been compromised?

According to the Verizon 2016 Data Breach Investigations Report, in 93% of cases, it took attackers minutes or less to compromise systems. Organisations, meanwhile, took weeks or more to discover that a breach had even occurred—and it was typically customers or law enforcement that sounded the alarm, not their own security measures.
90% of breaches, and 86% of incidents, are covered by just these patterns.

Miscellaneous errors

Any unintentional action or mistake that compromises security, excluding the loss of assets. 26% of miscellaneous errors involved sending sensitive information to the wrong person.

Insider and priviledge misuse

This mainly consists of incidents involving misuse by insiders. Attacks are typically motivated by money (34%) and espionage (25%), such as the theft of intellectual property.

Physical theft or loss

The loss or theft of laptops, USB drives, printed papers and other information assets. The biggest threat of a data breach is from lost or stolen documents, which cannot be encrypted.

Denial of service

The use of botnets—a "zombie" army of computers, typically taken over without the owner's permission—to overwhelm an organisation with malicious traffic. DoS attacks can bring normal operations to a halt, causing chaos.

Malware

Malicious software that infects one's computer - such as viruses, worms, Trojan horses, spyware and adware.

Web-app attacks

Where a web-app, such as a CMS or e-commerce platform, is used as the means of entry. Financial services, retail, and information industries are most effected.

Point-of-sale intrusions

When attackers compromise the computers and servers that run POS applications, with the aim of capturing payment data. Accommodation and retail are most effected.

Phishing or spoofing

Fake emails, text messages and websites created to look like they're from authentic companies. They're sent by criminals to steal personal and financial information from the user and are often presented in a manner than seems official and intimidating, to encourage one to take action.

How can we help?

Grant Thornton can assist to assess the readiness of your organisation to handle, recover from and respond to a cyber security incident, including both public relations and business resilience aspects.

Organisations need to anticipate and have proven strategies to effectively respond to disruptive events caused by cybercrime, maintain critical operations and learn from events to better prepare for future challenges. By partnering with us and using our wealth of experience, we can coach organisations to face the challenges that these disruptive events create.

We have identified 5 key assessments to help you address your security concerns. Our assessment consists of iterative processes that emulate the approach of an attacker exploiting vulnerabilities.

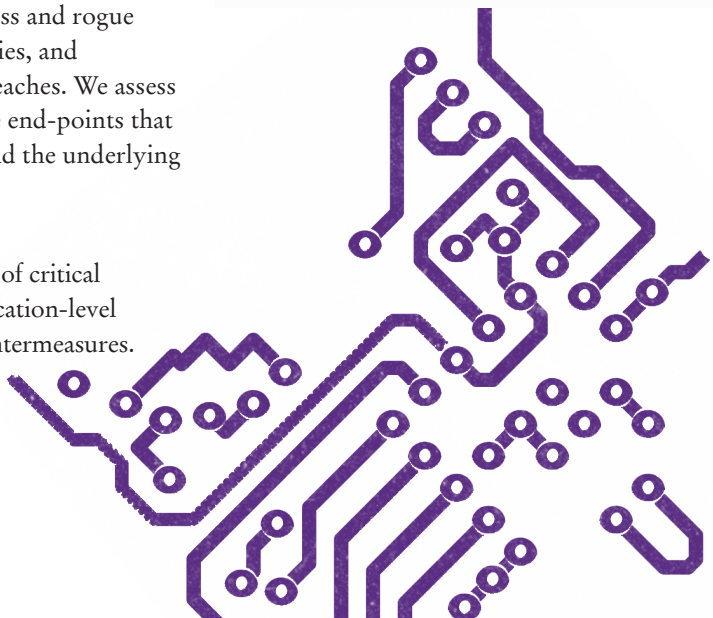
- **External vulnerability assessment and penetration test**
  This phase involves identification of as many security vulnerabilities in an organisation's network that are accessible from the internet. This type of assessment targets a company's externally visible servers or devices including e-mail servers, Web servers or firewalls. The objective is to find out if an outside attacker can get in and how far they can get in once they've gained access.
- **Internal vulnerability assessment and penetration test**
  This is the identification of security vulnerabilities that are accessible from inside the organisation. The focus is to identify the breadth of potential security issues on systems that are accessible from within the network, emulating a threat from an internal resource, such as an employee, contractor, or business partner.
- **Web application assessment and penetration test**
  This is the identification of security vulnerabilities on a web-based application. The focus is to identify the use of insecure coding practices, security flaws in the application design or misconfiguration of the application and supporting services.
- **Wireless network assessment and penetration test**
  A wireless network penetration test identifies areas of weakness and rogue devices, analyses security configurations, tests for vulnerabilities, and implements security policies that minimise risk of security breaches. We assess the configuration of your wireless infrastructure as well as the end-points that connect into it, the authentication and encryption controls, and the underlying logic used to connect into the wireless infrastructure.
- **Security configuration assessments**
  A host security configuration assessment evaluates the security of critical servers. We analyse administrative and technical controls, application-level security issues, and propose specific recommendations for countermeasures.

63%

of confirmed data breaches involved leveraging weak, default or stolen passwords.

(Source: Verizon 2016 Data Breach Investigations Report)

As more and more employees work away from the office – at home and on the go – and collaborate online, sensitive corporate information is increasingly leaked, often unintentionally.



Cyber security: our approach

Grant Thornton's cyber security and privacy team has significant experience in assessing, improving and embedding controls to better align exposure to risk appetite. We have worked with organisations of all sizes across all industries and can tailor our services to meet specific client needs across a wide range of topics, including cyber security, cyber crime, digital security, vendor assurance and data privacy. Our methodology revolves around four main steps - preparation, protection, reaction and change.

PREPARE

Common client questions:

- **What should we do if we don't fully understand our existing vulnerabilities?**
- **What should our information security strategy look like?**
- **How do we know if our organisation meets all of its obligations for information assurance?**
- **What should we be asking third party organisation when we consider partnering with them? How do our existing third party service providers affect our susceptibility to cyber attacks?**

We help you understand your current exposure to cyber-security risk and support you to develop an effective security capability.

Our services include

- **cyber-security risk and threat assessments**
- **security policy development**
- **security process or technical assessments**
- **third-party cyber-security assurance.**

PROTECT

Common client questions:

- **What should our cyber governance andv controls look like?**
- **How do we identify and repair system vulnerabilities?**
- **How can we improve the security of information we store in the cloud?**
- **How can we design our processes to minimise security risks?**

We develop and implement the technical framework and broader processes required to protect. We can help you with:

- **security architecture**
- **security architecture**
- **security technology implementations**
- **security process design and implementation**
- **identity and access management**
- **privacy and data protection**
- **data classification**
- **enterprise application integrity**
- **business continuity and disaster recovery**
- **penetration testing.**

Small and medium-sized businesses are just as much at risk as large enterprises.

New data from Symantec's 2016 Internet Security Threat Report shows that about 1 in 40 small businesses are at risk of being the victim of a cyber crime. That pales in comparison to the 1 in about 2 large businesses which are targeted every year - multiple times - with a cyber attack.

Training is key

Grant Thornton Malta has worked with leading industry experts and its international Grant Thornton partners to develop courses to help businesses better understand online threats and how to protect business data, money and reputation.

The training is relevant to staff and owners in a wide range of businesses, from sole traders to large companies and is aimed at empowering them to better understand information security risks and how to protect against fraud and cyber-crime.

REACT

Common client questions:

- **Does our organisation have a response protocol in the event of a cyber attack?**
- **What should we do if we don't have the necessary capability to respond to a cyber attack?**
- **What are our options if a third party breach exposes our customer data?**
- **Can our existing systems adapt to meet new regulations and/or standards regarding the security and privacy of data?**
- **Is it possible to recover from internet worms, malware, or trojans that take over workstations and systems?**

We work with you to support and monitor your cyber-security operations, and help you to respond rapidly and forensically in the event of a security or data breach.

CHANGE

Common client questions:

- **How can we raise awareness of cyber risks throughout the organisation and in the boardroom?**
- **How do we demonstrate the return on investment of our cyber security measures?**
- **How do we instil a cyber-secure awareness in our company's culture?**

We can help you improve and better manage your cyber-security capability.

Our services include:

- **security programme strategy and planning**
- **security governance security awareness.**

Your contact

Joe Pullicino
Partner
Business Risk & Outsourcing

M. 00356 9949 9660
E. joe.pullicino@mt.gt.com

Grant Thornton
Suite 3, Tower Business Centre,
Tower Street, Swatar, BKR4013 Malta
T. +356 2132 0134
E. grantthornton@mt.gt.com

Grant Thornton
An instinct for growth™

© 2017 Grant Thornton Malta. All rights reserved. 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 Malta is a member firm of Grant Thornton International Ltd (GTIL). 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.com.mt