Grant Thornton

An instinct for growth™

Cyber crime incident response and investigation

April 2019

Cyber crime incident response and investigation

The Cyber Tsunami

Cyber-crime is affecting organisations of all sizes and increasing in impact and complexity every day.

Social media, big data, AI and cross-connectivity means that the ever increasing volume of data we hold can be immensely valuable, providing insight and analytical opportunity to grow your business and improve your customer relationships.

However, with the privilege of holding data comes the obligation to do so "appropriately", demonstrating that you have considered and implemented appropriate technical and organisational measures to keep that data safe. And yet despite the threats of enormous fines, more than capable of wiping out a business for a single data breach, studies show that over 25% of businesses still lack basic tools to detect an ongoing data breach. [1]

Planning and Preparedness

Good cyber risk consultancy can help reduce the risks of attackers penetrating the "perimeter" defences of your business, your firewalls and malware detection systems for example. However, cyber incidents can have many faces and can include malicious as well as accidental human and insider risks, alongside technical failure, misconfiguration, supply chain and third party risks – among a myriad of ever evolving threats. While good perimeter defences and effective controls are the foundation of good cyber security, they are not a guarantee against a cyber incident.

Effective preparation has been proven to dramatically decrease the impact of a cyber-attack, with the most significant reduction coming about through the implementation of an incident response function, followed by effective data governance and employee education.

Integrated Support

Grant Thornton's Cyber Incident Response Team is available to support your business in the event of a cyberattack or data loss event. We work alongside your existing IT and Legal teams to provide a co-ordinated, timely and efficient investigation and remediation.

Our team includes incident responders with world-class training and experience providing hands-on support to a wide variety of organisations, large and small, local and international.
Our team deploy the very highest standards, techniques and technologies, operating with our state-of- the-art ISO 27001 accredited laboratories. Our team are experienced in making regulatory reports to the Information Commissioner's Office, the FCA, SFO and others within the UK and internationally.

Proven Expertise

Our experts are well versed in dealing with a range of responses, from a minor loss of an unencrypted USB stick to sophisticated organised criminals seeking to exfiltrate over $100 million from a client bank.
Our experts are well versed in dealing with a range of responses, from a minor loss of an unencrypted USB stick to sophisticated organised criminals seeking to exfiltrate millions from an organisation. Our maturity and experience is well recognised in this space.

We provide the full range of services to help your stakeholders understand the data assets they hold and to help secure them in the event of a cyber incident. Expert computer forensics, incident response planning and training, and around-the-clock crisis response capabilities provide you with comprehensive organisational security.

[1] 'GDPR News: UK data watchdog opens GDPR helpline for 'SMBs', ITPRO, 31/05/2017: www.itpro.co.uk/dataprotection/28029/gdpr-news-uk-data-watchdog-opens-gdpr-helpline-for-smbs/page/0/1

Protect and detect

Respond and resolve

Threat and risk assessment
Incident readiness, threat simulation

Incident response planning
Robust IRP, Governance and staff training/ communications

Response, Investigation and reporting
Initiate IRP, investigate root cause, report to relevant parties

Remediation
Confront reasons for incident and establish new normal

Normal operations

Incident preparation

Respond to incident and identify cause

Stakeholder management

Cyber incident preparedness

Incident Readiness

Our incident readiness review takes best-in-class industry standards such as ISO 27035 and applies them to your organisational plans and infrastructure to assess how your business is placed to respond to cyber incidents.

We can review your existing cyber security assessments including third party penetration tests and vulnerability scans (or help to conduct them if you have not done so already), existing Incident Response Plans and general organisational security to help identify gaps in people, processes, policies and technologies. We can test the robustness of your existing infrastructure through a spectrum of non-invasive or invasive exercises including red and blue team exercises.

We report to you on key areas of improvement including technical integrity, procedures upon discovery of the incident, coordination of the response team and identification of critical stakeholders and their duties. These reviews can be conducted through the lens of computer forensics or alongside your existing GDPR implementation. We are also highly experienced in working with internal legal teams and external counsel to help align our work to your regulatory obligations.

Cyber Threat Simulation - War Gaming

A simulation is typically carried out as part of a wider incident readiness review. Also known as 'war gaming', this exercise will typically include your senior management and members of the IT team.

Through detailed pre-assessment of your environment we prepare a realistic simulated scenario that will test a variety of your infrastructural and operational postures. This simulation takes place through a multi-hour exercise and a variety of evolving scenarios, encompassing challenging business continuity and reputational and legal concerns for your teams.

The simulation is designed to:

- Develop effective lines of communication among key stakeholders
- Provide challenge and training to senior management and employees
- Highlight deficiencies in the response that can be addressed to improve future capabilities.

An Investment in Security

Our cyber simulation concludes with a formal feedback or a report highlighting strengths and improvement opportunities.

An independent and objective assessment of your organisational response can help provide evidence under the "Accountability Principle" of the GDPR, demonstrating an investment in "proportionate governance" aimed at minimising the risk of a data breach.

Technical checks - Penetration Testing

During the scope of our Breach Response investigations our team can conduct network security and penetration tests in order to determine whether and how your environment was compromised.

Our specialists have a range of tools at their disposal that can be deployed to test your technical assets. These include specialist log and artefact analysis tools, allowing us to undertake an accelerated assessment of months or years of historical data to help identify intrusions, weaknesses and behavioural anomalies.

Incident Response Plan

The most critical component to have in place in order to be better prepared for cyber incidents is an Incident Response Plan (IRP). We can work with you to develop a robust IRP that can be used in the event of a cyber incident and to help shorten the impact and cost of an incident through effective identification, containment and future mitigation.

Ensuring that the correct team is in place and roles and responsibilities have been identified within the plan is crucial. This plan will typically provide structure and division of labour between:

Incident Management Lead

- IT
- Legal
- PR
- HR
- Internal Audit
- Data breach resolution including client communications
- Forensic support.

Regulatory reporting requirements need to be identified, and planning should be in place to support this.
Public and internal communication plans and statements can be prepared in advance to help avoid panic and misstatement in a crisis.

Third Party and supply chain liabilities are often overlooked and we support you with conducting supply chain data risk audits.

From May 2018 the GDPR requires a mandatory report of a data breach within 72 hours of the event, and carries fines of up to 20 million Euros or 4% of group worldwide turnover. 18% of businesses surveyed believe a fine of this size would be likely to put them out of business.

Cyber Insurance

Cyber Insurance increasingly provides a practical cost shifting option and can help address the costs of preparing for and responding to a cyber incident, although not the fines that can flow from failure to respond appropriately.

Our Cyber Incident Response Team are highly experienced in working with Insurers and Loss Adjusters in pre- and post-incident response and helping reduce risk and premiums through effective preparation.

Governance and Investigation

Governance

We can work with you to raise awareness at C-suite level of the level and impact of cyber incidents within your business. This involves developing understanding of the current level of preparedness and any improvements that need to be made for cyber incident readiness. We provide strategic recommendations based on industry standard best-practice and our experience working with your peers.

Investigation and Root Cause Reviews

We can conduct independent root cause reviews and investigations into cyber incidents in order to determine the origination. Such reviews are often required post-incident to help defend criminal and civil liability, and to help support insurance and loss adjusting processes.

Our specialists are trained in chain of custody requirements and civil procedure rules and are widely experienced in presenting evidence as expert witnesses. We have undertaken reviews and provided evidence in claims worth hundreds of millions of pounds.

Our reviews typically encapsulate the following:

- The key operational IT control environment which should have operated in respect of the incident and the components or processes which precipitated the failure
- The IT security management and data governance arrangements and how they operated in these incidents
- Resilience, incident management and disaster recovery responses taken
- The role of outsourced and offshore/cloud IT relationships
- How the direct implications of the incident were managed, including prudential and conduct implications if a financial services organisation.

We draw on the skills and experience of our Forensic & Investigations team to provide robust reports using rigorous investigation techniques and support reporting to regulators, prosecuting authorities and insurers.

Incident response

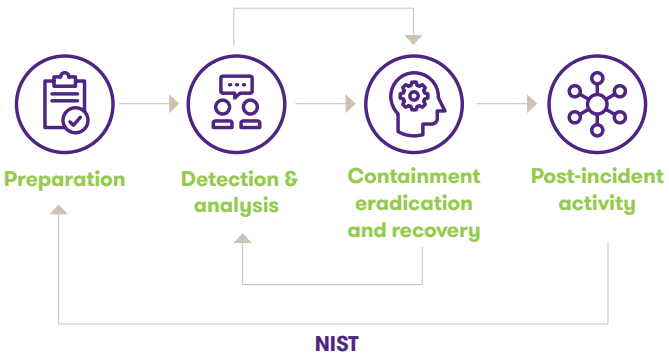
Preparation with your team will minimise the time required to contain and investigate the incident.

We provide an incident response service that will seamlessly integrate into your IT function and wider business. Integral to this is a hotline number to contact our team, with supporting email cirt@cy.gt.com rapid response during business hours.

Our team can also engage separately to support operational and infrastructural cyber resilience including the development of a Security Operations Centre and live, real-time threat detection and response.

Our typical response protocol follows the NIST and ISO 27035 best practises:

- Following a call to our helpline or team, we will respond to provide immediate support in identifying the nature of the issue (eg is it ransomware, lost data, phishing email etc.)
- We will work with your support team to consider an appropriate response for containment, investigation and mitigation of the incident:
  - This work may include the immediate remote collection of data logs and forensic imaging of impacted systems
  - We will assess whether our team is most effective physically on the ground or working remotely
  - We will begin work immediately and in parallel to contain and investigate the incident
  - Our team will work closely with your senior management team and IT team to effect a mitigation strategy and appropriate recovery protocol
  - Mitigation may include severe options such as taking services offline and rebuilding data environments and so will require appropriate access to and consideration by senior stakeholders
  - We conclude our work with a written summary of the incident including appropriate lessons learned and mitigation recommendations for the future.



For further information, please contact:

Christos Makedonas
Managing Director
Technology Risk Services
T +357 22600000
E Christos.Makedonas@cy.gt.com

grantthornton.com.cy