Grant Thornton

An instinct for growth™

Cyber incident management

Are you prepared for a cyber failure?

What are the challenges?

Cyber based services touch almost every part of our professional and private lives, with increasing dependency. As our reliance grows, organisations need to be prepared for outages and have plans in place to restore business as usual. It is important to understand these risks and implement appropriate controls to protect IT infrastructure and services.

A cyber incident is one where systems, networks or IT services have been breached, either through malicious attack, technical failure, human error or misconduct. While strong perimeter defences and effective controls are the foundation of good cyber security, they are not a guarantee against a cyber incident.

Organisations should have robust incident management processes in place to protect their data, clients and reputation in the event of an outage. These should be integrated with crisis management, business continuity and IT disaster recovery arrangements.

Failure to prepare may create the following impacts:

- Reputational damage – high profile incidents can be embarrassing and may lead to loss of client confidence and a drop in share value.
- Compromised client information and confidential data – leading to potential personal distress for clients and loss of sensitive company information.
- Legal implications – relating to the Data Protection Act or the upcoming General Data Protection Regulation (GDPR).
- Regulatory censure or fines – inadequate controls may lead to large fines or trading restrictions.
- Business disruption – business as usual may not be possible, leading to immediate financial losses.
- Increased operating costs – the initial cost of dealing with a major cyber incident is estimated to be between £30k-£40k in the first 48 hours.

Cyber response planning

- **Data mapping**
- **Adequate security controls and penetration testing**
- **Related policies and procedures**
- **Breach response team procedures and contingency planning**
- **Cyber insurance**
- **Scenario testing**
- **Audit**

Case study:
Cyber incident management following a ransomware attack

Our banking client received a ransom email, as opposed to traditional ransomware. We provided initial crisis management support and investigated the incident further. Unbeknownst to our client, the cyber criminals had built an entire virtual infrastructure over several months and had used this to attack the organisation from the inside. We contained the infection and confirmed the source and duration of the attack. Our experts helped to restore business operations and advised our client on how to minimise reputational damage.

[1] Cyber Security Breaches Survey 2017 by Ipsos Mori and the University of Portsmouth, commissioned by the Department for Culture, Media and Sport

Our Integrated Incident Management approach

In the event of a cyber incident, it is easy to focus the investigation on what happened, at the expense of managing the full spectrum of the impact, including business disruption. We have adopted an innovative approach to cyber incident management, addressing the full range of issues.

Our Integrated Incident Management (IIM) response methodology aims to understand the event and proactively manage it to reduce the impact. Once the situation is under control, we examine the root cause and identify lessons to be learned to reduce the risk of similar incidents occurring in the future.

Incident preparation

Adequate preparation and robust incident response plans form the first step towards effective crisis management. These should be supported by crisis training for senior management and scenario testing, as appropriate.

Establishing the facts

The next step is to identify what happened, which systems are affected and whether the issue concerns the network or a single computer. Other considerations include the sensitivity of the affected system, the potential for litigation and which communication channels have been compromised.

Stabilising the situation

The ultimate goal is to prevent further damage. This may require a range of forensic services to collect evidence in the case of legal and regulatory proceedings. However, sometimes simply securing the system needs to take priority.

Business continuity and preventing reputational damage

It may be difficult to make an informed decision during an event, due to the timescales involved, and business continuity plans provide a useful blueprint. Cyber incident management should form a key part of any business continuity plan.

Preliminary report

The findings will be presented in the form of a preliminary report in plain English. Bespoke recovery and remediation recommendations will include a clear analysis of the risks and benefits of each approach, helping management decide the next course of action.

Recovery and remediation

Once the issue has been neutralised, the system will be restored to its operational state and tested extensively to ensure it is functioning correctly. The system will also be monitored for a set period of time after the incident, with any complications addressed immediately.

Final report

A final report will be produced, detailing why the incident occurred and how future risk can be minimised moving forward. This will be supported by a bespoke prevention strategy which considers performance, existing processes and cost effectiveness.

Improvement

The prevention strategy will be implemented across the firm, which may include updating policies, additional staff training or installing new technologies.

How can we help?

Many cyber incidents may be averted and we can help to secure your organisation and reduce your risk. In the event of a breach, we can help you minimise the impact to facilitate an effective business recovery. Our extensive range of subject matter experts can guide you through each stage of the IIM response.

Cyber incidents are inherently complex in nature and require specialist, diverse skill sets to resolve. Each incident will have unique characteristics and challenges, and no single person will have all the necessary skills for the most effective response. We have staffed our incident response team with an appropriate breadth of skill sets and proven experience, to help your business recover from a cyber incident.

We can help you prepare for these challenges through:

- Cyber risk and threat identification and assessment
- Network and system vulnerability assessments and penetration testing
- Business continuity and IT disaster recovery benchmarking and planning
- Data landscape mapping and privacy assessments
- GDPR compliance assessment and remediation work
- Incident and crisis management programme assessments, development and improvement
- Incident and crisis management support services
- Cyber-crime investigations, evidence preservation and gathering services
- Incident root cause analysis reviews and reporting
- Staff training and awareness
- Incident response exercising, testing and wargaming

For further information, please contact our team below:

Sandy Kumar
Chair of Financial Services Group
Head of Business Risk Services UK
T +44 (0)20 7865 2193
E sandy.kumar@uk.gt.com

Manu Sharma
Director
Business Risk Services
T +44 (0)20 7865 2406
E manu.sharma@uk.gt.com

Kev Brear
Senior Manager
Business Risk Services
T +44 (0) 207 865 2425
E kev.brear@uk.gt.com

Vijay Rathour
Partner
Digital Forensics Group
T +44 (0) 207 184 4684
E vijay.rathour@uk.gt.com

Grant Thornton
An instinct for growth™