Grant Thornton
An instinct for growth™

Cyber Security

Incident response

Why Grant Thornton?

In the era we live in, no business can afford to be lax about cyber threats. Unlike most forms of crime, illegal hacking is extraordinarily profitable and involves very little risk for the perpetrator. There are entire companies and departments of government in every part of the world dedicated solely to finding and exploiting soft targets. Grant Thornton can make sure you are not a soft target. We offer a full spectrum of services developed to manage all manners of threats:

1. Respond

- prepare organisations to respond to security incidents;
- assist the response to data security breaches;
- forensic investigations;
- litigation support;
- 24/7 incident handling; and
- discovery and evidence management.

2. Assess

- evaluate security across the enterprise;
- understand the security of new technologies, regulatory audits, data protection and privacy;
- understand security risks and threats; and
- assess security by breaking it - penetration testing.

3. Improve

- develop and implement a security strategy;
- develop security policies and procedures;
- implement security technologies and processes;
- raise cyber security culture and awareness;
- vulnerability assessment;
- information security consulting;
- staff training; and
- drills, scenarios and campaigns.

We respond to dozens of IT security incidents every month worldwide. We have dealt with everything from simple virus infections, web-site defacements and email hacks to the very largest cyber frauds and international hacking incidents. We help our clients validate, assess, contain and remedy cyber incidents with the minimum of disruption, publicity and cost.

Our incident handling process

1. Identification

The first thing any incident investigator needs to do is ascertain the nature of the incident. Is the issue occurring across a global network or isolated to a single computer? How sensitive is the system concerned? Is there a potential for litigation? What communication channels may be compromised? These and many more questions like it are the kind we will help you answer. This allows us to focus our efforts and swiftly get to the root of the issue.

2. Validation and assessment

Once we have a better idea of how to approach the problem, the next step is to start the investigation. This involves us collecting as much pertinent information as possible and sifting through it to discover the root cause. Hopefully this will be a benign and easily-rectifiable issue, but in some cases our findings will indicate something more malicious is at work.

3. Preliminary report

At this point, we will present our findings to you in a concise and easy-to-digest manner. Making the right decisions during an incident is paramount, so we go to painstaking lengths to make sure you have the best possible intelligence. We will tailor our recommendations to suit your needs, and give you a thorough analysis of the risks and benefits of each approach.

4. Containment

At this point the ultimate objective is to prevent any further damage. If necessary, we can perform the full suite of forensic services to ensure any evidence collected will stand up to scrutiny in court. In a time-critical emergency, the decided approach may prioritise kicking an attacker out of the system as soon as possible. When dealing with sensitive scenarios involving high financial risk, containment will need to be more delicate and nuanced. Our priority will always be what is best for your business.

5. Recovery and testing

Once the system has a clean bill of health, our objective is to ensure everything is back the way we found it. We will work with your team through a gamut of tests to make sure the system is functioning perfectly. Even after all checks are passed, we can monitor the system for a period afterwards. If any complications arise, we'll be able to catch them promptly.

6. Final report

When everything is back under control, we collect up our notes and findings and create a presentation for you. This breaks down how and why the incident occurred and the ways that damage can be mitigated going forward. Through careful analysis we can devise a bespoke prevention strategy that will balance performance, convenience and cost effectiveness appropriately. Our cyber security experts will then work with your company to implement and manage any necessary changes.

How can we help you

At Grant Thornton we can handle any cyber incident to which Irish and international organisations are vulnerable. We have responded to:

- control systems hacks;
- ransomware infections (opportunistic and targeted);
- data thefts (by insiders and outsiders);
- email frauds;
- denial of service attacks;
- website hacks;
- network breaches;
- phishing/fraud site take downs;
- telecommunications systems hacks; and
- systems interruptions.

Our dedicated cyber security team coordinates Grant Thornton International's worldwide incident response capability. We provide expert and technical support to our cyber incident first-response teams in every continent.

We maintain incident response teams in a number of countries. We can and have deployed specialists from these countries to many others and provided online support to incident responders in dozens of countries. Some of the countries we have worked with include:

Key contacts for our dedicated team include:

Mike Harris
Partner, Cyber Security
T +353 (0)1 436 6503
E mike.harris@ie.gt.com

Andrew Harbison
Director, Forensic and
Investigation Services
E andrew.harbison@ie.gt.com
T +353 (0)1 680 5766

Offices in Dublin, Belfast, Cork, Galway, Kildare, Limerick and Longford.

www.grantthornton.ie @GrantThorntonIE Grant Thornton Ireland

Grant Thornton
An instinct for growth™

grantthornton.ie