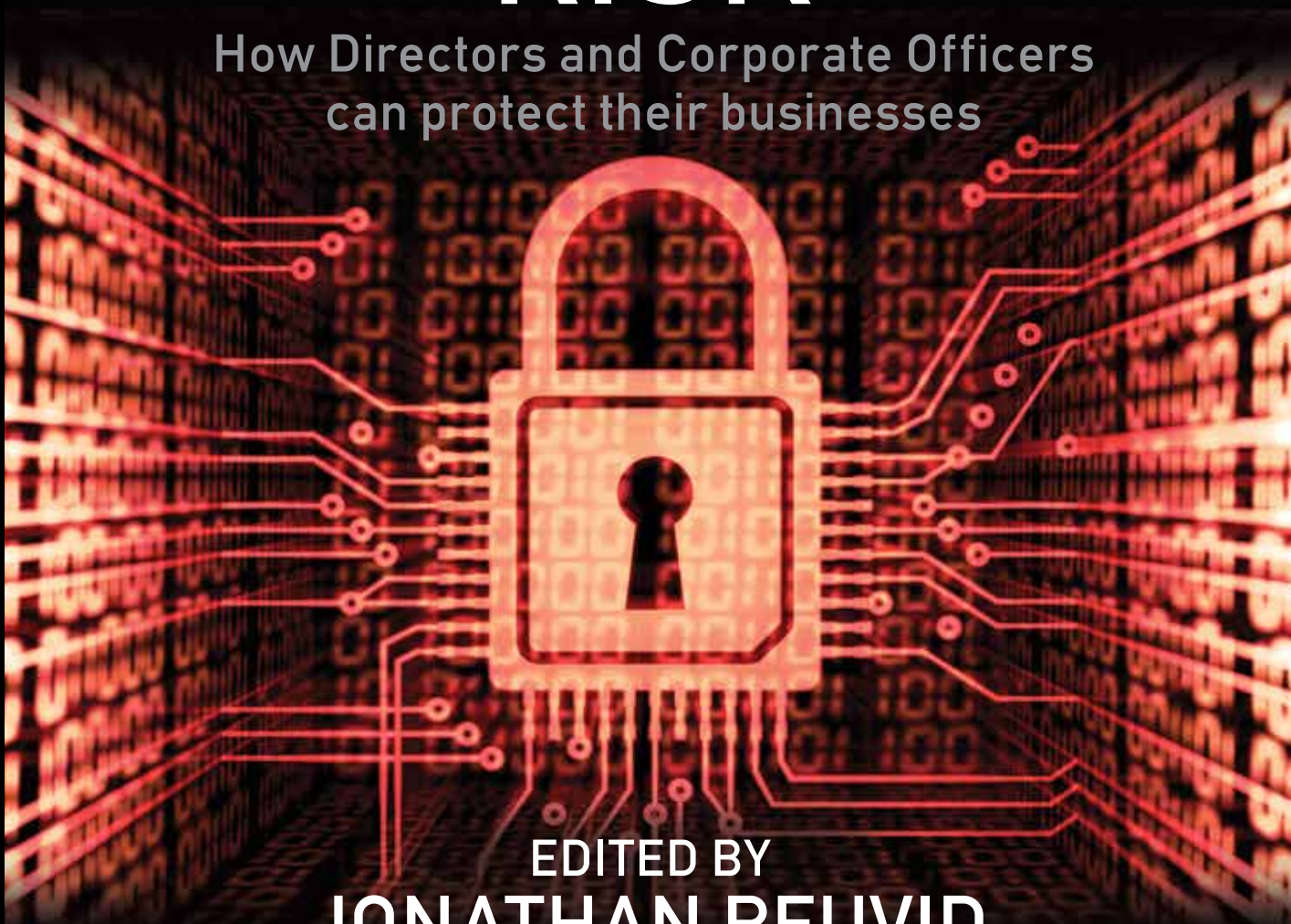
MANAGING CYBERSECURITY RISK

How Directors and Corporate Officers can protect their businesses



EDITED BY

JONATHAN REUVID

accenture

DLA PIPER

AXELOS GLOBAL BEST PRACTICE

BAE SYSTEMS INSPIRED WORK

MANAGING CYBERSECURITY RISK

How Directors and Corporate Officers can protect their businesses

EDITED BY
JONATHAN REUVID

Legend Business

5.1
MANAGING CYBER INCIDENTS AND INTERNAL SECURITY BREACHES

Julian Cracknell, BAE Systems Applied Intelligence

INTRODUCTION

As cyber hackers become more sophisticated and the volume of attacks escalates, it is almost inevitable that every organisation will at some stage experience a cyber attack or breach. In response to the continual and evolving cyber threat, all organisations need to ensure that their defensive measures are equipped to deal with the threats that they are facing. However, securing end-points and digital perimeters with firewalls, intrusion detection and data loss prevention is no longer enough. It is now just as important to mitigate against the consequences of a breach.

In a recent survey that BAE Systems conducted with large enterprises, over 57 per cent of respondents had experienced a cyber attack in the previous 12 months, with a quarter experiencing a breach in the previous month. Cyber criminals are getting smarter, sharing resources and ideas. They understand what tools are available to prevent their attacks, engineer their tactics accordingly and persevere with long term strategies until they are successful.

The impact of an attack can be devastating; stolen intellectual property can destroy competitive advantage, breached customer data can extinguish millions in profits and abuse of data privacy can attract unwanted scrutiny and fines from regulators, while damaging reputations. Our research indicates that the direct cost

of dealing with a cyber attack for a large company is on average over £330,000, and can reach over £1 million. This doesn't include the reputational or brand damage and the consequent impact on revenues. The real impact is likely to be considerably higher.

Whatever a hacker's background and motivation, if they are suitably driven and skilled, they will get into almost any network. With comprehensive cyber defence in place, a large proportion of attacks can be stopped. However, this means that those who do penetrate the network are determined or talented enough to present a serious threat, and consequently a comprehensive strategy is required to defend an organisation in the event of a breach.

The first step in the battle to mitigate damage is to be prepared. Recent research shows that only 29% of businesses have formal written cybersecurity policies and only 10% of businesses have a formal incident management plan.[1] For such a plan to be effective it needs to be regularly tested, with lessons identified and its measures updated and enhanced. Only half of respondents' organisations had tested their incident response plan in the previous six months.

Managing the response to a cyber incident is a complex task that involves the coordination of many resources, tasks and information. Events and threats must be understood. Decisions must be taken. Technical measures must be deployed. Further damage must be avoided. Stakeholders must be kept informed. Evidence must be preserved. Lessons should be learned. All of this will be conducted under intense time pressure and scrutiny. Preparation before the event allows organisations to focus on their strategic response rather than being caught in the web of competing tactical decisions.

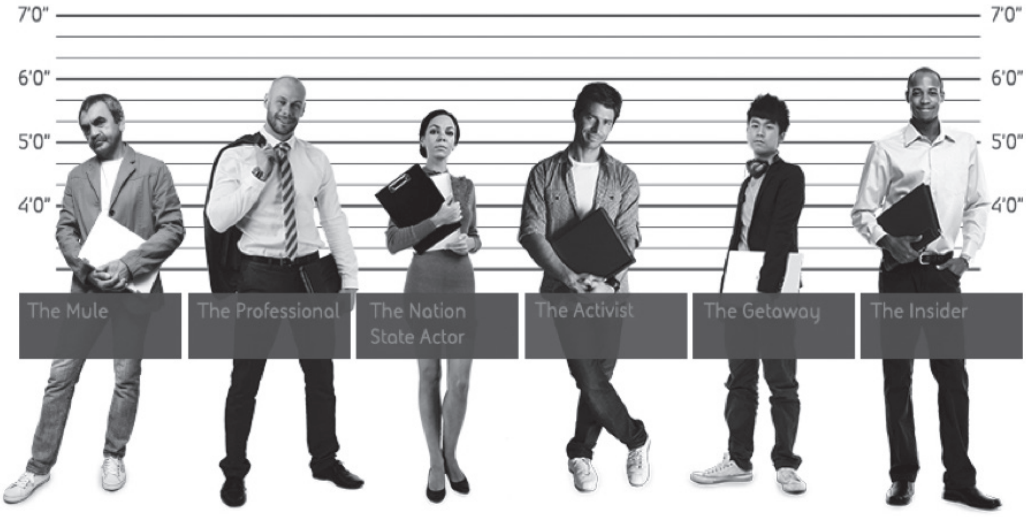
WHO SHOULD I BE WORRIED ABOUT?

Attackers fall into several categories, illustrated in Figure 5.1.1, that we have labelled *The Unusual Suspects*.[2] Each attacker has a different motivation and is likely to require different strategies to counteract.

1 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf

2 http://www.baesystems.com/en-uk/feature/the-unusual-suspects

Figure 5.1.1 The Unusual Suspects



The categories are:

- ***The Activist:*** These hackers take their political, social or ecological views seriously enough to want to make a public statement out of their hack. They may not be as organised as other attackers but they will aim for maximum publicity of the breach – which will discredit the targeted organisation, as well as steal sensitive data.
- ***The Getaway:*** Too young to go to prison, these attackers 'get away' with a reprimand. They are likely to have basic hacking skills used to impress peers and get noticed by more serious hackers.
- ***The Insider:*** Difficult to identify, the Insider may be a disgruntled or negligent employee or commercial spy. Inside the organisation, they can bypass security controls, copy data removable media or drives or install malware.
- ***The Mule:*** A casual criminal or opportunist, the mule is used by others to launder the proceeds of a hack. The most vulnerable to detection and arrest, the mule turns cyber crime into 'real money'.
- ***Nation State Actor:*** Often working for a business that is bankrolled by or connected to those in power. Goes to great lengths to cover their tracks and can severely inhibit organisations.
- ***The Professional:*** Works at what looks like a '9 to5' job, but is a risk-averse career hacker. They may run a botnet, be part of a criminal cyber gang or sell cyber crime tools to others.

Each of these attacker profiles presents different risks to an organisation and are likely to demand different strategies to deal with them. Types of attacks can range from data breaches, such as Wikileaks or Sony Pictures, financial fraud such as the recent Bangladesh Bank heist, a Distributed Denial of Service (DDOS) website attack such as the BBC experienced or simpler malware attacks. Any incident response readiness strategy must account for multiple perpetrators and scenarios and deal with each appropriately.

FAIL TO PREPARE, PREPARE TO FAIL

> "When a successful cyber-attack occurs and the scale and impact of the breach comes to light, the first question customers, shareholders, and regulators will ask is, 'What did this institution do to prepare?'" - Mckinsey[3]

There is no one-size-fits-all incident response readiness strategy – no two incidents or organisations are exactly the same. The response plan must be tailored to each organisation and consider a variety of incidents as well as types of attackers.

In order to be able to respond to the full range of cyber attacks, organisations should adopt a comprehensive strategy that covers the approach to: People, Process, Tools and Awareness.

People

- ***Authority:*** Clearly assign roles and responsibilities for key executives accountable for managing the incident. Include escalation routes, board sponsorship and communications schedules. Consider the impact of making business critical decisions; the nominated executives must have the knowledge and experience to implement changes to critical business systems. Board level sponsorship is crucial for success of the overall plan.
- ***Resource:*** Ensure the right skills are available, regardless of the time or day of the week – hackers don't just work to a 9-5 timetable. Don't be overwhelmed by the attack – ensure additional resources are accessible to handle day-to-day tasks to keep the business running. It's important to maintain business as usual as far as possible. Sometimes hackers can carry out diversionary tactics by setting off one smaller hack on the network that diverts all the resource and attention, while the hacker attempts a much bigger attack elsewhere. Third party specialists can help with monitoring complex scenarios or if there is a surge of simultaneous attacks.

3 http://www.mckinsey.com/business-functions/business-technology/our-insights/how-good-is-your-cyberincident-response-plan

- ***Practice:*** As well as adopting a thorough incident response readiness plan, conduct regular incident response rehearsals and penetration testing. Test exercises in crisis response handling should be co-ordinated across the organisation – from IT to HR, communications, finance and PR – and ensure that the complexity of decisions required in the event of an attack are understood. Simulating a real event will help to build awareness and experience within the team, increasing their effectiveness when a breach occurs.

Process

- ***Process:*** Make this defined and accessible to everyone across the business. One of the main shortfalls of an incident response strategy can be the failure to communicate the plan across the business before an attack. Include guidelines and checklists and regularly re-evaluate them to ensure relevance. Another area for failure is siloed strategies, especially in global businesses. Business units often develop their own incident response plans; these work well in highly targeted attacks but are unhelpful during sustained company-wide incidents.
- ***Legal:*** Legal consultation may be required during an incident. Maintain data logs and adapt processes in accordance with law enforcement, particularly relevant for internal breaches where logs would be required as part of an insurance claim or court proceedings. Specific data may be required to prove an employee is violating contractual obligations in order to terminate employment. If the attack is in the public domain, evidence may be required to reassure customers and other stakeholders that all actions were taken to mitigate against risk and appropriate procedures were carried out once the attack occurred.
- ***Reporting:*** Damage limitation is not confined to the network and ICT systems. Construct a hierarchy of organisations, stakeholders and customers that need to be informed of the breach, including the media. Senior management will require extensive knowledge of the attack to ensure the correct information is relayed at the right time. Regulators may also require information following an attack; for example telecommunications companies are required by law to disclose any information regarding a data breach. Even for organisations that are not legally bound to publically declare an attack the reputational damage of failing to declare a breach that is subsequently made public can be significant. A clear reporting process can avoid many of these issues.

Tools

- ***Evidence:*** Maximise logging with sufficient storage on all devices, such as firewalls, proxies and active directory servers. If an attack is suspected, then avoid installing new software to collect data as it could alert the attackers and cause

them to conduct diversionary tactics. Additionally, don't take infected machines offline until the threat is fully understood – this evidence may be required should the case go to court, or for other litigation or regulatory reasons.

- ***Investigation:*** Devise a priority matrix to help triage and understand the *who*, *what*, *when*, *why* and *how* of the attack. Consider all possibilities, discovery of unknown unknowns and the root cause of the attack to defend against attacks elsewhere on the network. Verify what has been taken without making any assumptions. Network and disk forensics as well as malware analysis and attribution can assist, as well as third party forensics teams.
- ***Remediation:*** Applying remedial actions across the estate should be done as rapidly as possible – with risks weighed up for more drastic actions, such as website or network closures – if necessary. Take into consideration any evidence required and the ability of the organisation to continue business as usual. Closely monitor the corrective actions to ensure success – it is likely that a hacker may have been inside the organisation for weeks or even months and therefore is unlikely to simply accept being locked out. They may see responses as a challenge and take action to implement even more damage. Instigate recovery from backups where required and ensure constant and consistent oversight of the networks to prevent repeat attacks.

Awareness

- ***Threat Aware:*** Intelligence related to the attack methods and perpetrator can be used to initiate the appropriate response, improve remediation tactics and understand the severity of an attack. Adapt the response to the typical threat behaviours for more rapid recovery. The *Cyber Security Breaches* survey states viruses, spyware and malware are the most common forms of attack at 68% with impersonation of organisations at 32%, so devise strategies for these threats first.
- ***Impact Aware:*** The business implications of an attack can be devastating, not just on the organisation that is breached, but on customers, supply chains and stakeholders. Evaluate the impact of business critical decisions while minimising the impact of the attack. For example, if networks are taken offline, what is the risk to the rest of the business, how many staff are able to function, and what is the risk to customers and profits?
- ***Context Aware:*** Sophisticated hackers conduct reconnaissance about when sensitive information such as financial statements or new product launches are due for release. The hackers may have infiltrated the network for months before they attack, which will give them the potential to cause the most damage. Increase awareness of specific targets and times of greater sensitivity, and enhance monitoring and detection capabilities to mitigate against the risk of an attack.

Establishing and communicating an incident response readiness strategy will reduce the opportunity for mistakes, limit the impact of an attack and ensure greater chance of the right evidence being available, should it be required.

EXECUTING THE STRATEGY AFTER AN ATTACK

Figure 5.1.2

The first hours after an incident has been detected are the most critical. Whether alerted by an anti-virus alert, a tip off from an external party or suspected inside activity, the response should be immediate. It can be perilous to ignore anything that concerns possible cyber attacks.

The immediate aftermath is the best opportunity to capture data about the hack and use this threat intelligence to ensure the appropriate response is coordinated effectively. With an incident response plan in place, execution becomes a more strategic and less frantic job.

We recommend a five step execution plan, characterised by the image in Figure 5.1.2, as part of the emergency response in the immediate hours after detecting a breach.

Step 1: Confirm
Before escalating the incident, verify all the information available at the time without making assumptions. What is the status of the network and what, if any, data has been accessed? Immediate action must be taken to protect the remaining data and network while simultaneously ensuring evidence is preserved. Mitigate as much risk as possible at this early stage and assess the risk versus benefits to any major network decisions. Consider whether escalation is required at this stage, including management of media and stakeholders.

Step 2: Capture
Ensure all evidence of the breach is recorded by maximising logging on multiple devices across the network. Explore the incident, particularly if specific stolen data appears online. Gathering as much data as possible in the early stages can deliver threat intelligence and help dictate the effectiveness of the response. At this stage

third party experts may be called upon to deploy network probes and host agent software to give remote access to the network and help gather evidence.

Step 3: Expose
The full range of discovery techniques should be applied, such as forensic tools, behavioural log analysis and reverse malware engineering. It is crucial to understand who is conducting the attack, whether it is a group, a state or an individual; where the attack is coming from, internally or externally, and what the attackers did while inside the network, including any data that has been taken or exposed online. Fully briefing board members and informing the media is appropriate at this stage. Don't under or overplay the scenario, keep to the facts and remediation techniques being deployed to overcome the situation.

Step 4: Remediate
With the intelligence already gathered and analysed, the most effective method for inhibiting the attack and recovering the infected components should be deployed. This may not be the most drastic action available, and could simply be the removal of the malware while maintaining current systems. If an insider attack has occurred it could be to take the suspected individual offline and investigate further before blocking them from the network.

Step 5: Resume
Continue to monitor the network for further attacks and to ensure the hacker has been removed. Scrutinise social networks in the aftermath for any new data and consider inspecting outside networks, such as the cloud networks used by hackers to dump information, to ensure no further data leakages occur. Review the incident response readiness plan and adapt according to lessons learned.

CONCLUSION

There are two types of organisation: those that know they have been hacked and those who don't. With the average time taken to detect a breach now at more than 100 days, this observation has never been truer.

Despite the best efforts from the world's best security teams, breaches occur and data is regularly exposed. There is no silver bullet when it comes to handling an incident, internal or external. The winners in this war will be the ones who prevent an attack as much as possible in the first instance, detect the hack as early as possible and have a cast-iron strategy for rapid response and damage limitation.

APPENDIX I
CONTRIBUTORS' CONTACTS

Accenture New York
1345 6th Avenue
New York, NY 10105
Tel: +1 917 452-8982
Contact: Chris Thompson
e-mail: chris.e.thompson@accenture.com

AXELOS Global Best Practice
17 Rochester Row
London SW1P 1 QT
Tel: +44 (0) 207 960 7865
Contact: Nick Wilding
e-mail: Nick.Wilding@AXELOS.com

BAE Systems Applied Intelligence
Blue Fin Building, 4th Floor
110 Southwark Street
London SE1 0TA
Tel: +44 (0) 203 296 5900 Contact:
BAE Systems Marketing e-mail:
learn@baesystems.com

DLA Piper UK LLP
3 Noble Street
London EC2V 7EE
Tel: +44 (0) 207 153 7714
Contact: Sam Millar
e-mail: Sam.Millar@dlapiper.com

Boolean Logical Ltd
20-22 Wenlock Road
London N1 7GU
Tel: +44 (0) 780 308 5249
Contact: Nick Ioannou
e-mail: nick@booleanlogical.com

Cyber IQ
IQPC, Floor 2
129 Wilton Road
London SW1V 1JX
Tel: +44 (0) 207 3689 334
Contact: Richard de Silva
e-mail: Richard.De.Silva@iqpc.co.uk

Cyber Rescue Alliance
4 Bonhill Street,
London EC2A 4BX
Tel: +44 (0) 207 859 4320
Contact: Kevin Duffey
e-mail: kevin.duffey@cyberrescue.co.uk

Legend Business Books Ltd
Legend Times Group
107-111 Fleet Street
London EC4A 2AB
Tel: +44 (0) 207 936 9941
Contact: Jonathan Reuvid
jreuvidembooks@aol.com

Oakas Ltd
Wessex House
Teign Road
Newton Abbot
Devon TQ12 4AA
Tel: +44 (0) 207 127 5312
Contact: Richard Preece
e-mail: richard.preece@oakas.co.uk

Don Randall Associates
44 Fitzwalter Road
Colchester
Essex CO3 3SX
Tel: +44 (0) 7836 275 484
Contact: Don Randall
e-mail: donrandallassociates@gmail.com

Raymond Romero
Federal Reserve Board
Washington, DC 20551-0001
Tel: +1 (0) 202 369 9379
e-mail: Raymond.romero@frb.gov