Global Investigations Review

The Guide to Cyber Investigations

Editors
Benjamin A Powell, Leah Schloss, Maury Riggan and Jason C Chipman

The Guide to Cyber Investigations

Editors:

Benjamin A Powell

Leah Schloss

Maury Riggan

Jason C Chipman

Reproduced with permission from Law Business Research Ltd
This article was first published in June 2019
For further information please contact Natalie.Clarke@lbresearch.com

GIR
Global Investigations Review

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK

www.globalinvestigationsreview.com

Enquiries concerning reproduction should be sent to: natalie.clarke@lbresearch.com.
Enquiries concerning editorial content should be directed to the Publisher:
david.samuels@lbresearch.com

ISBN 978-1-83862-223-7

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

Acknowledgements

BAKER MCKENZIE

BCL SOLICITORS LLP

CLIFFORD CHANCE US LLP

COVINGTON & BURLING LLP

RICHARD DENATALE

HUNTON ANDREWS KURTH LLP

KROLL, A DIVISION OF DUFF & PHELPS

BRIAN MCDONALD

QUINN EMANUEL URQUHART & SULLIVAN, LLP

ROPES & GRAY LLP

WILMER CUTLER PICKERING HALE AND DORR LLP

Publisher's Note

The Guide to Cyber Investigations is published by Global Investigations Review – the online home for all those who specialise in investigating and resolving suspected corporate wrongdoing.

It aims to fill a gap in the literature and provide an in-depth guide to every aspect of preparing for and dealing with data breaches and other cyber incidents. These incidents can be challenging, to say the least.

As such it is a companion to GIR's larger reference work, *The Practitioner's Guide to Global Investigations* (now in its third edition), which walks readers through the issues raised, and the risks to consider, at every stage in the life cycle of a corporate investigation, from discovery to resolution.

The Guide to Cyber Investigations takes the same holistic approach, going through everything to think about before, during and after an incident. We suggest both books be part of your library – *The Practitioner's Guide* for the whole picture and *The Guide to Cyber Investigations* as the close-up.

The Guide to Cyber Investigations is supplied to all GIR subscribers as a benefit of their subscription. It is also available to non-subscribers in online form only, at www.globalinvestigationsreview.com.

The publisher would like to thank the editors for their energy and vision. We collectively welcome any comments or suggestions on how to improve it. Please write to us at insight@globalinvestigationsreview.com.

Contents

Part I

A 'Typical' Cyber Investigation

1

The Cyber Threat Landscape

Jason Smolanoff, Alan Brill and Andrew Beckett[1]

Introduction

Hackers, cybercriminals, ransomware, cyberterrorism, state-sponsored cyberespionage, hacktivism: we hear these terms constantly. Cyber incidents have become newsworthy because virtually everyone's personal data has been compromised in one or more of the thousands of incidents that have occurred over the years, only some of which have been made public.

Every system that uses digital technologies – whether it involves centralised servers with immense processing power and storage capabilities or information we store and transact on our smartphones – has vulnerabilities associated with it. Some of these are well known and understood; others are constantly emerging. The reality is that a system that was considered secure yesterday may be insecure this morning because a new, previously unknown hardware or software issue (called a zero-day vulnerability) has been identified.

Systems are compromised by attackers for many reasons. A disgruntled current or former employee with a grudge wipes out a key file or program. A nation-state actor compromises a company's competitive bidding system and provides its forthcoming bid to a competitor in its country. A hacker compromises huge numbers of payment card accounts and offers them for sale on the dark web. A criminal tricks someone at a help desk into providing them with access codes. A misconfigured system allows an intruder to go from a portion of a system that monitors environmental conditions in one location to one that stores sensitive financial information. These all have happened and continue to happen.

In this chapter, we share our collective insight spanning the public and private sectors, different parts of the world, and diverse industry backgrounds and experience of more than 40 years investigating and responding to cyber incidents.

1 Jason Smolanoff and Alan Brill are senior managing directors and Andrew Beckett is a managing director at Kroll, a division of Duff & Phelps.

The questions we cover are: Who are the suspects? What kinds of threat-actors are out there targeting our systems? Is there some logic in how they select victims? In how they attack? Why are so many attacks successful?

Breaking down the problem

Cyber incident actors: who are they?

Who are the actors behind cyber incidents? While there is no universally accepted list, and while a perpetrator can be part of multiple groups (however those groups are defined), experience indicates that there is a broad taxonomy we can use to bring some ordered thinking to the question of who is carrying out attacks and why they select their particular targets.

Nation-state actors

Nation states have recognised that cyber is a domain of warfare that is inherently asymmetric; that is, a small number of talented people can have a huge effect. In the Ukraine, for example, Russian hacking was believed to be responsible for substantial power outages. A nation state can act directly or indirectly.

Direct actions of nation states

This is the case when a government is directing the actions of people carrying out an attack. Examples of agencies believed to have offensive cyber capabilities include the US National Security Agency, the Russian Main Intelligence Directorate (GRU), the People's Liberation Army of China, and governments as diverse as North Korea (Democratic People's Republic of Korea) and Israel. They have employed cyber operators who act for the nation state under the direction of their superiors.

Outsourced actions of nation states

A nation state may lack capacity in terms of qualified hackers but still want to carry out offensive cyber operations. In these cases they may decide to outsource the work and can consider a range of possible actors. They may contract with civilian criminal hacking groups with the requisite capabilities or work through an allied country that has the capabilities. They may also act through a non-government group. For example, it has been reported that during the 2016 US presidential campaign, Russian organisations hacked the Democratic National Committee, but used the Wikileaks organisation to release and distribute the stolen material.

Non-state or quasi-state actors

There is also a range of non-government organisations (NGOs) that may be behind offensive cyber activities.

Terrorist activities

Terrorist groups have become sophisticated users of cyber capabilities. They may use the internet for recruiting, financing, information theft or distribution. They may carry out operations to confuse their enemy, appearing to have greater or fewer numbers of personnel than they really do. Cyberterrorism has become a field of study in itself.

Information anarchists

We have seen the growth of organisations (some loosely organised) that believe no information should be secret, or at the very least, those they target should have no secrets. They may steal emails or other information and post it publicly. They may strike out in various ways, including distributed denial of services (DDoS) attacks designed to take a target website out of operation.

NGOs who share a common cause with state actors

Do not think that every attack can be attributed to one of the aforementioned types of operators. Just as threats can involve multiple risks, multiple actors can operate in concert (either formally or informally). They may share a target (but operate independently) or may coordinate their efforts; for example, a nation-state actor steals the data, but an NGO distributes it.

Organised cybercriminal organisations

Organised cybercriminal organisations can, aside from their own for-profit operations (e.g., stealing sensitive personal information, credit card data, health insurance data and the like), be the source of malware or they may provide malware as a service offering. They may also engage in other forms of attack (e.g., DDoS). They will provide their services to anyone who pays them. We are seeing an increase in the use of 'professional' malware in attacks. This makes it hard to determine attribution because, while the attack may have been seen before, it does not tell you who the attacker is. It also puts sophisticated attacks in the hands of , or at the direction of , less sophisticated attackers; what looks like organised crime may still actually be attributable to a disgruntled employee or a nation state. There have also been reports of groups such as street gangs or criminal motorcycle gangs turning to cybercrime as a source of funds.

Individual cybercriminals

Individual criminal actors can carry out attacks that may be indistinguishable from those of organised criminal gangs. They may also offer their services to others (malware as a service, DDoS as a service, etc.) in return for a fee. The availability of pre-packaged attack software (i.e., ransomware toolsets) makes today's cybercriminal far more dangerous than those of former years.

Investigative journalists

In the past, journalists used hacking techniques to pursue stories, but the spread of cybersecurity and anti-hacking laws has made this practice dangerous. Particularly in the United Kingdom, the phone intrusion trials that resulted in journalists and editors being convicted and sentenced to prison have curtailed these practices.

Insiders

Disrupters

There are insiders who are on a mission to cause problems for a company. It could be a disgruntled current or former employee. It could be someone who gets themselves hired (or assigned as a temporary employee) to gain access for the purpose of causing problems. A

motivated disrupter with appropriate access can cause tremendous damage. For example, a disrupter who is in an IT position could cause backup files to be replaced with useless files, and could then damage live files that have no usable backup. This is why monitoring software that can detect suspicious or unauthorised activities is so important.

IP compromiser

An IP compromiser has a mission of stealing intellectual property (IP). IP can be valued at millions or even billions of dollars. Stealing a software source code can jump-start a foreign competitor's capabilities.

Data compromiser

Like an IP compromiser, a data compromiser is up to no good. He or she wants to steal data that can either be turned into money (for example, by selling it to a credit card number distributor) or released, directly or indirectly, to embarrass a target organisation.

Unintentional

Insiders can also be responsible for incidents without intending to do so. They can also be divided into two broad groups: victim and error maker.

Victim

An insider can be targeted by a perpetrator to take an action to help carry out an attack without realising that they are doing so.

- Phishing: Phishing emails have become ubiquitous. They have the objective of getting the recipient to either click on a link within an email that leads to the deployment of malware, or to give up log-in credentials, credit card numbers or other valuable data. Even though some organisations offer anti-phishing training to employees, this scheme still works on a small percentage of the targeted population.
- Social engineering. Criminals will use the phone to induce an insider to reveal non-public information. In one method, the caller pretends to be from the company's IT department and needs to log in remotely to fix a problem, which requires getting the employee's log-in credentials. Some people fall for it and provide the information.
- Business email compromise. A perpetrator sends an email to a targeted employee, sometimes using an email address very similar to that of the targeted organisation, pretending to be a senior executive. The bogus senior executive needs the employee to help with a secret deal by wiring funds (sometimes millions of dollars, or the equivalent) to a specific account. Most people now recognise this for the fraud that it is, but sometimes it works, and the funds are transferred.
- Work-at-home dupe. An individual can be induced to take part in what they believe to be a work-at-home opportunity that turns out to be part of a sophisticated theft scheme. The work-at-home worker may turn out to be supporting money laundering, sanctions evasion or other crimes.

Error maker

Sometimes, an individual simply makes a mistake that leads to a data compromise. For example, a systems developer may inadvertently misconfigure a cloud-based storage container and leave it open to access through the internet, leading to the data stored in the digital container being compromised. Similarly, something as simple as an email sent to an incorrect address (or a fax message sent to the wrong fax number) can cause the compromise of highly sensitive information. This can be caused by accidentally entering the wrong email address, or deliberately (but unknowingly) directing an email to an address set up by an adversary with a very similar address to that of the real organisation.

Scanners

It is important to point out that cyber perpetrators may also use automated tools to look for companies whose systems exhibit particular vulnerabilities that leave them open to attack. Thus, a company may be targeted simply because the attacker has the capability to successfully carry out an attack. These attacks use tools called scanners that, in effect, test sites for the presence of specific weaknesses that render the site vulnerable to penetration.

Cyber incident methods

High-tech, low-tech and blended attacks

It might be easy to throw up one's hands and say that data breaches are inevitable and, to an extent, that is true. There is no such thing as 100 per cent security but that is not an excuse to give up. Any meaningful study of threats recognises that some are high-tech. They rely on vulnerabilities in software or in cybersecurity operations. Others are low-tech, relying on human error. Still others combine multiple vectors of attack into blended threats. Consider the following examples.

Vault 7

Vault 7 is the name given by Wikileaks to its trove of cybersecurity information apparently stolen from the US Central Intelligence Agency. Vault 7 material included what were previously unreported methods for compromising multiple types of systems. Suddenly, with the release of Vault 7 material, nation states and cybercriminals had access to world-class hacking tools. This is one reason for so many attacks being successful. They employed methods that the perpetrators would have never had access to if it were not for the release of CIA materials through Vault 7.

Polymorphic malware

When malware was first developed, defensive systems were developed that could recognise the specific signature of particular pieces of malware. But malware writers understood this and developed what is called polymorphic malware, which modifies itself every time it is duplicated, without the changes affecting the functionality of the malware. Once each copy is unique, traditional pattern-based detection systems cannot see it. Newer defensive tools had to be developed to recognise the actions of the malware. Adversaries continue to develop malware with more advanced detection-avoidance capabilities, so anti-malware vendors are always in a race to keep pace.

Malware (and malware as a service)
Tens of thousands of pieces of malware are developed every day. Malware can be aimed at an operating system or a particular application. The proliferation of malware makes it vital to maintain up-to-date patching. Patches are software modifications developed by manufacturers to counter specific threats, including those associated with malware. Additionally, as a business feature, some malware writers, rather than selling a piece of malware to a buyer, operate it for them, and this is known as malware as a service.

Ransomware (and ransomware as a service)
In the past couple of years, a new form of malware called ransomware has emerged and been the cause of tremendous problems for both public and private sector organisations. When it enters a system, ransomware encrypts storage devices that it can control, leaves behind a notice that the software has encrypted stored documents and files, and informs system owners that upon payment of a ransom (often to be paid in a cryptocurrency such as bitcoin or monero), the perpetrator will send a decryption key. While initial ransomware usually asked for a few hundred dollars, ransomware today is often targeted at enterprises, and ransom payments ranging from tens of thousands to hundreds of thousands of dollars may be demanded. High ransom payments are often demanded if the ransomware has the capability of encrypting cloud-based backup copies of files. Unfortunately, many companies feel they have no alternative but to pay the ransom and have to hope that the criminals will actually provide a working decryption key. Note also that some ransomware is provided to criminals as a service operated by other criminals. Some are so sophisticated as to provide detailed instructions for the victim to use in purchasing cryptocurrency. Some even provide a customer service phone number for victims to call for payment assistance.

Denial of service attacks
Websites can be overwhelmed by receiving millions of messages per second. This is how DDoS attacks work. Most often operated by criminals as a service, these attacks take advantage of thousands of computers that have been infected with malware that enables them to be commanded to send large numbers of messages to a target. With hundreds or thousands of computers sending large numbers of messages to the target, the website can be disabled. These DDoS attacks can be combined with a blackmail demand ('Pay me and I will stop the attack') or may be conducted for political or ideological purposes. Fortunately, internet service providers have become good at defeating these attacks.

Social engineering
Social engineering attacks focus on making people do what the attacker wants. The many forms include the following:

- Business email compromise, as discussed earlier.
- Credential compromise. This is a scheme designed to get a targeted individual to reveal system credentials, such as user ID and password. One way of reducing the chance of a successful credential compromise is to use what is called two-factor authentication (or 2FA), whereby a user ID and password is not sufficient to gain access to a system. The second factor could be a message sent to a smartphone, or a fingerprint, or any number of other means.

- Dropping infected drives. Perpetrators have been known to leave a thumb drive containing malware where it can be readily found. For example, it might be left attached to a key ring in a public toilet, or in a company car park. The hope is that it will be found and the drive plugged into a computer in an attempt to identify the owner (perhaps by finding a picture or document with a clue as to the person's identity). Once plugged in, the drive injects the malware into the system, where it is designed to spread. An alternative is for someone with access to the premises, such as a janitor, to plug an infected drive into multiple computers.

Automated attacks

One method that perpetrators use to identify potential victims is an automated attack, in which the perpetrator uses software that runs tests against target systems to identify those with specific vulnerabilities. In some cases, the objective is to identify a vulnerable system for infection at a later stage. In other cases, identification of the vulnerability is combined with exploitation of the vulnerability.

The life cycle of an attack

Attackers must overcome a lot of challenges before their efforts can be considered successful. Of course, this involves some understanding of the objectives of the perpetrators. For example, if the objective is to render a given website or internet-connected access point unavailable, the attacker does not have to figure out how to access, collect and extract data from the target. Rather, the attacker needs to know only how to either block access to the site or cause it to fail. For example, if a site's manager has not taken simple (but vital) steps to prevent unauthorised changes to the internet registration of a domain (e.g., sampledomain.com), an attacker can initiate a transaction that could associate that domain name with an internet protocol address controlled by the attacker. When someone enters the domain name, they end up somewhere else. Once the objective of the attack is known, the elements of information needed to understand the attack become evident.

While attacks against cyber infrastructures have been going on for more than 50 years in various forms, there are many published standard ways of defining how incidents occur. Some, we have found, oversimplify an attack and do not result in the depth of understanding needed to understand why an attack was successful, what worked (and did not work) for the attackers, and what you need to know to effectively strengthen your cyber defence measures. In developing this chapter, we decided to use the MITRE ATT&CK™ model,[2] which is the result of contributions from many experienced practitioners as a way of describing attacker behaviours in a consistent way.

The ATT&CK model suggests that to fully understand an incident, an organisation should try to understand the following characteristics of attacker behaviour. Our experience indicates that it is unlikely that all these characteristics will be known, particularly at the initial stage of an incident response and investigation, but it is a very useful model for reminding the investigators of the diverse avenues they need to pursue.

2 The MITRE ATT&CK model is both a database and a model for understanding the ways in which cyberattackers operate. It is available for use without charge. See https://attack.mitre.org/resources/getting-started/.

Initial behaviour

How was the attack initiated? Did it involve removable media? Was it a 'drive-by' (a visit to a website that automatically downloads malware)? The result of a phishing email? Social engineering? Additionally, attackers may carry out pre-attack activities such as surveillance (i.e., determining what tools are in use within a network and testing to determine whether common exploitable vulnerabilities exist). Recognising these indicators of an attack that is in the planning stage can help an organisation to prevent it, or at least to mitigate the damage. Note that pre-attack activities can be either focused on a specific target or carried out by automated systems to create a list of vulnerable sites to be exploited in the future. This element of the incident includes what some other models refer to as 'reconnaissance activities'. To the extent that a network can detect these types of activities, that can be an early indicator of a potential attack on the network, and can provide the information needed to prevent or mitigate a successful attack and exfiltration of data.

Execution

What was the technology used to initiate the compromise? Was it a compiled HTML file? Did it use a dynamic data exchange? Was PowerShell used?[3]

Persistence

In previous decades, the attack model was to get in, steal data, cover your tracks and get out quickly. Today, the model has morphed to one in which the attacker aims to establish a long-term stealthy presence in the target network. This characteristic describes the means used to support persistence of an attack.

Privilege escalation

Once an attacker enters a system, they may well need to gain additional capabilities to do things like getting to valuable data, moving to other parts of the system, establishing persistence or being able to remove data from a network. How they go about doing this is described in this characteristic.

Defence evasion

Once in a system, attackers do not want to be noticed, caught or prevented from carrying out their plans. They understand not only that their targets will put defences in place to prevent them from being successful, but what those defences are likely to be. There are many ways in which an attacker can bypass or otherwise evade these defensive measures; understanding how they carried out the evasion is an important part of understanding the attack as a whole.

Credential access

How did the attacker get the credentials used in an attack? Did they find the information in an insufficiently protected file? Was a known vulnerability used to gain access to a valid credential? Was the attacker able to cause the creation of a credential that was not supposed to exist?

3 PowerShell is an automation engine and scripting language with an interactive command-line shell that Microsoft developed to help IT professionals configure systems and automate administrative tasks.

Discovery
How did the target discover the attack? For example, did they notice a strange device on their network? An unusual file? An anomalous movement of data out of the system? Unfortunately, the discovery process may not start until the victim organisation is notified of the attack by a third party (e.g., by law enforcement agencies or a payment card issuer).

Lateral movement
Once an attacker has gained access to a network, how do they navigate from one part of that network to another part of the network, or to a connected network? As an example, in the well-known 2013 attack against the retailer Target, the cybercriminals first entered the system through a vendor responsible for store heating and cooling systems; they were then able to move laterally through the network to gain access to the payment card information of tens of millions of customers. Moving from the environmental systems part of the network to the payment card portion of the network represents lateral movement.

Collection
What techniques were used by the attackers to collect the data that they intended to move out of the system? Were they able to access shared drives? Did they use screen captures? Did they access information stored on a remote system (i.e., cloud storage)? Understanding this is key to developing more effective defensive measures.

Extraction
How did the criminals get the data from your network to the site or email address that they control? Did your data leakage control system fail (if you have one)? Were there unprotected endpoints? In one case, we discovered that an organisation that believed it had 14 points of connection to the global internet actually had more than 70!

Command and control
There are a number of ways in which an attacker can monitor and direct an attack against an organisation. As with other categories, understanding how they achieved command and control helps with strengthening defences.

In looking at this list, you may notice that there was no specific element focused on the identity of the perpetrator of the incident. There are several reasons for that. First, once it is determined, for example, that the attack was designed to steal credit card information and that the stolen information was transmitted to a site in Asia, there may be little or no value in spending time and money in what may well be a fruitless search for the identity of those responsible. The chance of actually catching them and bringing them to justice is low, and an insurer or managers may not want to incur that expense. Second, there are many ways in which a perpetrator can obfuscate its connection to your data. You may believe you know who the perpetrator is, but that may not be sufficient to support a prosecution or to result in an international extradition.

Monitoring the threat environment

Is there a requirement to monitor the threat environment? We believe that organisations have an obligation to understand the risks they face. Without such an assessment, an organisation cannot effectively target the resources available to them to maximise their protection, and some may require assistance in monitoring for threat intelligence and active threats. There are many sources – commercial, government, academic and not-for-profit – that may be able to provide assistance in this regard.

Threats are constantly evolving along with technology. Business risks that were acceptable yesterday may be unacceptable today. New threats are constantly arising. Simply carrying out a threat assessment is not enough; the process must be constantly reviewed to take into account threat evolution. But in addition to threats posed by nation-state actors, NGO actors, insiders and hacker groups, an organisation's freedom of action in regard to self-defence may also be affected by laws, regulations, contract provisions and self-interest. These may require or prohibit certain actions by an organisation to accomplish cybersecurity goals.

Law

Governments worldwide are recognising the risks associated with cyber operations in their public and private sectors, and passing laws to criminalise certain actions. These laws may extend to movement (or limitation of movement) of data across national borders. Organisations are responsible for maintaining knowledge of laws in countries in which they operate or in which their customers or data reside.

Regulation

Regulations, like laws, can affect decisions about how systems are structured and protected. As with laws, it is incumbent on companies to maintain knowledge of applicable regulations. Note that regulations can be promulgated by or limited to a single nation, or may be associated with a multinational organisation. For example, the EU General Data Protection Regulation has effect throughout the European Union.

Contractual

Some cybersecurity requirements can be the result of a contractual relationship. For example, on a global basis, those organisations accepting payment cards (debit and credit cards) are obliged by contract to protect card information using the Payment Card Industry Data Security Standard.

Self-interest

An organisation may set rules that are more strict than those required by law, regulation or contract. Having more limitations on data protection and movement than are required by external factors may be important in some industries, and companies are free to self-impose restrictions as long as those restrictions are compatible with laws, regulations and contractual requirements.

How to accomplish monitoring the threat environment

Obviously, organisations differ in size, technological capability, size of legal staff and needs. While some may have the in-house capability to monitor the nature of threats that they face, others may not. Regardless of these factors, the need to monitor the threat environment, to carry out risk assessment and to design, implement and maintain a commercially reasonable and effective cybersecurity program is incumbent on all organisations. Any organisation that lacks the capabilities to do so must seek assistance. In some cases, organisations may turn to government agencies for help with monitoring threats and developing and implementing an effective cybersecurity program, or they may seek help from academic institutions or not-for-profit organisations. But in many cases, the most cost-effective alternative is to work with a commercial vendor that can provide a continuing service to carry out monitoring, leveraging updated indicators of compromise and real-time notifications of problems.

Why are so many attacks successful?

We have been fighting challenges to our computer systems for almost 50 years, and challenges to our financial systems, intellectual property and informational targets with value for centuries. But it seems that as quickly as we develop defences, the criminals develop new ways of defeating them. Can we change that paradigm? And if we can, will we?

The root cause of the problem starts with the fact that the internet, as we know it, was never designed to be secure. It permits users to hide their identities. It allows for the creation of regions such as the deepnet or the darknet, which are invisible to most users and are employed in many cases for nefarious purposes.

We don't believe that the internet was created as it was with the intention of facilitating misuse. Rather, we believe that many – perhaps most – of the problems we face are a result of what is known as The Law of Unanticipated Consequences. This concept states that there can be results of actions we take that are not what we intended, and they can be either positive or negative. An unanticipated consequence can be the result of insufficient testing or simply not thinking in terms of negative (or positive) ways in which a piece of software could be used or abused.

Cyber investigations often involve identifying root causes that are unanticipated consequences. This should not be surprising. This aim of this book is to provide guidance in initiating, carrying out and reporting on investigations of cyber incidents. While most of the steps in an investigation are quite logical, sometimes investigative success involves thinking outside the box. In fact, it is the inability to think broadly that can be the cause of an investigative failure. Keep this in mind as you read and use this book.

Appendix 1

About the Authors

Jason Smolanoff
Kroll, a division of Duff & Phelps

Jason Smolanoff is a senior managing director and Kroll's global cyber risk practice leader. Jason has more than 19 years of experience in federal law enforcement and information security and has played a leading role in some of the most significant cybersecurity investigations in history. During his career, he has specialised in supervising and investigating sophisticated computer and network intrusions conducted by state-sponsored organised crime, hacktivists and insider threat actors, often developing and maintaining productive partnerships with international intelligence and law enforcement agencies as well as private industry.

Jason directs Kroll's global team dealing with cyber risk in both preventing incidents through risk management and dealing with incidents when they occur.

Jason served with the Federal Bureau of Investigation from 1999 to 2011. He was the Supervisory Special Agent for the Cyber National Security Squad, supervising special agents and intelligence analysts in responses to all aspects of complex national cybersecurity investigations with a nexus to counterintelligence and counterterrorism matters.

From 2010 to 2011, Jason was the lead mentor of the Organized Crime Unit, Major Crimes Task Force, in Kabul, Afghanistan. This role required significant liaison with numerous Coalition, Afghan and Intelligence Community partners from the United States, United Kingdom, France and Australia, as well as Afghan prosecutors and judges.

Alan Brill
Kroll, a division of Duff & Phelps

Alan Brill is a senior managing director and founder of Kroll's technology and cyber risk practice. Prior to joining Kroll, he was Director at the New York City Department of Investigation and a deputy inspector general in the New York City government. He was employed by Chase Manhattan Bank and Ernst & Young, and, in government, with the NASA Manned Spacecraft Center, Houston, on the Apollo moon landing project, and served

as a major in the US Army. He is an adjunct professor at Texas A&M University School of Law.

Andrew Beckett
Kroll, a division of Duff & Phelps

Andrew Beckett is a managing director and regional leader in Kroll's cyber risk practice. Before joining Kroll, Andrew served as head of Cyber Defense for Airbus Defense and Space. His prior service was with the United Kingdom's Government Communications Headquarters and the UN's Organization for the Prohibition of Chemical Weapons, where he was head of the Office of Confidentiality and Security. He is a visiting professor of cybersecurity at the University of South Wales.

Kroll, a division of Duff & Phelps
Kroll Associates UK
Nexus Place
25 Farringdon Street
London, EC4A 4AB
United Kingdom
Tel: +44 20 7029 5156
andrew.beckett@kroll.com

Kroll Associates, Inc
10100 Santa Monica Boulevard
Suite 1100
Los Angeles, CA 90067
United States
Tel: +1 424 249 1650
jason.smolanoff@kroll.com

Kroll Associates, Inc
2 Emerson Lane, Suite 200
Secaucus, NJ 07094
United States
Tel: +1 877 300 6816
abrill@kroll.com

www.kroll.com

Data breaches and similar incidents pose a unique challenge – those targeted must both respond and investigate simultaneously. It is an art that is impossible without preparation.

Businesses wishing to prepare will find this volume, *The Guide to Cyber Investigations*, invaluable. It identifies every issue to consider when creating a response template and implementing it, giving both the law and plenty of practical and tactical advice.

Written by leading contributors, all with broad experience of serious data incidents, it is an indispensable desktop guide and a worthy companion to GIR's larger volume on cross-border investigations, *The Practitioner's Guide to Global Investigations*.

Visit globalinvestigationsreview.com
Follow @giralerts on Twitter
Find us on LinkedIn

ISBN 978-1-83862-223-7