Deal Talk
Giving you the edge in Deals
www.pwc.co.uk/dealtalk

Buying a business?
Selling a division?
Merging organisations?
Refinancing your corporation?
Divesting part of a group?
Restructuring your portfolio?

Get our latest insight, analysis and opinion at www.pwc.co.uk/dealtalk

© 2014 PricewaterhouseCoopers LLP. All rights reserved. In this document, “PwC” refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.
Contents

Introduction 4
Foreword 5
The threats to private equity 6
Who conducts attacks? 8
How to minimise your exposure to cyber attacks 9
Conclusion 11
Introduction

Welcome to the BVCA *Guide to Cyber Security*, part of a BVCA series designed to serve as an introduction to important private equity and venture capital issues, investment strategies and markets. Our guides aim to provide a top-level overview of the latest trends and developments and provide a platform for further learning.

Produced in association with PwC, this latest entry concerns cyber security, an issue which increasingly affects everyone in a myriad of different ways. Whether you are a user of social networks, an online banker, a multinational corporation or a national government, cyber crime is now part of mainstream life. Security software specialist McAfee says that between £220 billion and £340 billion is lost to cyber crime each year, marking it a topic of huge importance to governments, businesses and investors alike.

Business has its own unique challenges. The rising threat from criminal groups and rogue nations to company reputation and profitability means protecting intellectual property and sensitive information is an everyday concern.

This is not easy, nor will it be getting any easier. A survey of cyber security experts by the Pew Research Center found that a majority believe cyber attacks are going to increase, with 61% predicting a major attack causing harm on a national level will occur by 2025. The situation is serious enough that the UK Government announced a £4 million programme to help small businesses counter cyber threats as part of the first-ever US-UK Global Cyber Security Innovation Summit in September 2014. The BVCA is also involved in the efforts to stem cyber crime with a place on the Cyber Security in Corporate Finance taskforce, run by the ICAEW in conjunction with the Cabinet Office.

This guide, as well as demonstrating the growing danger from cyber threats, presents a comprehensive overview of the various challenges businesses need to overcome and how to develop a coherent and robust cyber strategy.
Organisations are increasingly more reliant on digital business processes and applications to both operationally manage their businesses as well as deliver services to clients and customers. While technology-enabled advances provide a wealth of opportunities, they do also leave organisations vulnerable to very real cyber threats.

These attacks can impact any type of organisation and private equity houses should be equally as vigilant as corporates. A cyber attack or breach not only poses a risk to an organisation’s reputation but it is also likely to have financial consequences. PwC’s 2014 Information Security Breaches Survey found that the average cost to a large organisation of its worst security breach has increased from £450,000 to £850,000 in the period 2012 – 2103.

Larger organisations may be able to absorb these costs but if breaches go public it can gave have lasting consequences, affecting customer confidence and the bottom line. Take the American retailer Target Corporation. It suffered a breach in late 2013 which resulted in the theft of 40 million credit and debit cards data records in just three weeks, for example. The Washington Post reported that the company was expected to face fines in the region of anywhere between US$400 million to US$1.1billion.

For smaller organisations, however, the costs associated with a cyber breach may not be so easily absorbed, and in some cases can lead to situations from which recovery is impossible. These costs can be the result of significant data breaches as in the case of Target, but can also be caused by service disruption, theft of intellectual property or website defacements.

Often the financial and economic cost of an incident is unclear. In the case of targeted fraud or disruption, the financial impact might be immediate. In both cases, putting a final figure on the incident(s) is difficult when you consider opportunity cost and the impact on brand, reputation and consumer confidence. Where intellectual property is hacked and subsequently stolen, organisations may experience a slow decline in their value as their trade secrets show up in the products of competitors, potentially leading to a reduction in market share.

For private equity houses, these costs may have a broader impact. The financial and reputational damage as a result of a cyber breach can affect all those involved, from the private equity house to banks and investors. Understanding the range of potential attacks that may impact your organisation is crucial and will guide you when thinking about developing a robust security strategy.

This guide takes you through the cyber threats and risks faced by private equity firms and their portfolio companies. In particular, it will discuss critical steps in developing an effective cyber security strategy to help you protect what matters most and minimise the impact on your business.

James Rashleigh
Director, Cyber Security
PwC

“Seven out of 10 UK organisations experienced a security breach in the past year1. The UK Government also rates cyber security as a Tier 1 threat to the nation”

1 2014 Information Security Breaches Survey, Department for Business Innovation & Skills (BIS)
2 The UK Cyber Security Strategy – Protecting and promoting the UK in a digital world, UK Cabinet Office
The threats to private equity

Your structure and operations as a private equity house are unique, because of this you are susceptible to a variety of security threats. You must seek to understand both the threats to yourself as an organisation, as well as the threats that may impact the value of your investment portfolio. A private equity house can only effectively protect itself and the value of its investments from cyber attacks if it fully understands and responds appropriately to the risks and threats to which it is exposed.

Direct threats to private equity houses

Mergers and acquisitions
The cyber security threat around corporate finance transactions has already been recognised as a key issue by HM Government in a recent ICAEW report. M&A activity is a common target of espionage, ranging from corrupt competitors to foreign intelligence services. During the weeks or months leading up to a change in ownership, organisations on all sides of a deal face a heightened risk of cyber espionage from interested parties seeking to gain competitive advantage in the buying and selling process.

These attacks are not necessarily triggered by a related press release or announcement, and it is not uncommon for attacks to occur before any public announcement. It should be assumed that as soon as the idea of a merger or acquisition is discussed – even in private – there is a risk of a cyber breach, with the potential for a series of activities to undermine the merger or acquisition will occur. You may therefore wish to operate under the assumption you are at risk at all times, and put in place the necessary mitigations.

Financial information
Fraud may be opportunistic or planned, and can be targeted against individuals as well as businesses. Private equity houses are at greater risk than most businesses when it comes to higher value fraud attempts via cyber attacks. You are likely to hold financial and business information relating to your fund, your portfolio companies and your investors. All of this data has the potential to yield a high value return for an attacker.

“83% of espionage attacks focus on trade secrets”

Dilution of portfolio value
A cyber attack on an organisation in which a private equity house has invested can have a significant and lasting impact on the value of that business. If the value of an investment is impaired due to a cyber attack, it may impact the value of the portfolio, and in some cases you may need to consider an alternative or exit strategy. This risk is amplified if the portfolio is not diversified and focussed on a sector which is specifically being targeted.

Indirect threats to portfolio companies

It is difficult to assess the threats to a portfolio as a whole, and trying to identify which investments are most at risk of attack can be a daunting task. As a starting point it should be assumed that regardless of the type of data they hold, all organisations will be at risk from opportunistic attacks, including data theft and destruction or targeted fraud. Certain organisations are, however, more likely targets based on the amount of the data they hold and the sector in which they operate. Three key datasets, or types of information, that are known to increase the likelihood of an organisation being the target of an attack are:

Trade secrets
Trade secrets - including intellectual property, business intelligence and confidential communications - are all common targets of cyber attacks. In particular, organisations whose business is underpinned by the development of intellectual property are likely to be targets of espionage.

Private equity houses often invest in emerging technologies and new markets. Such companies have valuable trade secrets which, if stolen, could provide a competitive advantage to the receiving party. In the worst case it may result in the company going out of business.
**Consumer data**
Consumer data - including financial information and any personally identifiable information remains - a primary focus of cyber attacks. Organised cyber criminals employ a variety of methods to obtain such data, either to facilitate immediate financial gain or to acquire as commodities to sell on the black market. Retail organisations are at particular risk of this type of threat because they hold a large amount of personal data and payment card information. They are a primary target for organised criminals looking to steal financial databases to sell on the black market.

**Government assets or critical national infrastructure**
Organisations involved in the government and defence sector face a range of threats with different motives. Intellectual property theft is a permanent risk to most defence organisations, the threat being state-sponsored targeted espionage. Moreover, organisations involved in government or critical infrastructure are prone to hacktivists – those seeking to disrupt in order to raise an issue or prove a political agenda.

---

**Figure 4: Cross-border IPO activity 2013**

---

1. ICAEW Cyber Security in Corporate Finance, January 2014
2. 2014 Verizon Data Breach Investigations Report
Who conducts attacks?

Having an awareness of potential adversaries, understanding their motivations and gauging whether they are likely to attack can assist organisations in implementing the most appropriate methods of defence. The more aware you are of who is likely to attack you means you can develop an approach to cyber security that is informed and effective. You will be able to prioritise how to approach the different risks cyber threats present.

Categorising those behind cyber attacks can be done in many ways. One method is to divide them by motivation.

It is important to recognise that attacks not only originate from external sources. Insider attacks can also cause considerable damage to an organisation. Insiders often share one of the same motives as external attackers, although their reason may also arise as the result of injustice or discontent in the workplace.

<table>
<thead>
<tr>
<th>Attacker Type</th>
<th>Motivation</th>
<th>Description</th>
<th>Impact</th>
</tr>
</thead>
</table>
| Criminal      | For the money       | Cyber criminals seek to monetise their attacks. Common methodologies range from the distribution of malicious software that steals credentials to deploying ransomware that can be used to blackmail organisations or individuals to pay a fee to regain access to their own data. | • Costly regulatory inquiries and penalties  
• Consumer and shareholder lawsuits  
• Consumer confidence is undermined  
• Immediate financial loss |
| Hacktivist    | For the cause       | Hacktivists are motivated by a perceived cause. This type of threat receives most media coverage. They seek to disrupt services and/or deface websites to raise their profile, and to target those who go against their values. | • Disruption of business activities  
• Loss of competitive advantage  
• Consumer confidence is undermined |
| Espionage     | For the benefactors and their interests | Cyber espionage attackers try to steal specific information that can help further their economic and/or political objectives on behalf of their benefactors. Because there may be no immediate visible impact, espionage can go unnoticed for long periods of time. These attacks will often take the form of a targeted or Advanced Persistent Threat. These attacks are notoriously difficult to identify and remedy once found. They are usually targeted at individuals, activity is well hidden and the impact – usually theft of company data – can easily go undetected. | • Loss of competitive advantage  
• Erosion of portfolio value  
• Loss of negotiating position during a merger or acquisition  
• Disruption to critical infrastructure |
How to minimise your exposure to cyber attacks

You need to understand the risks you face as an organisation as well as the risks faced by those in your portfolio, and establish a plan to remediate any key gaps in your security posture. While technology is an area to consider, organisations need to take a holistic view of their structure and operations to truly appreciate their cyber exposure and threat landscape. Cyber security is not just about technology. It also involves people, information, systems, processes, culture and physical surroundings.

Understand your risk

Taking this perspective, private equity houses should take an integrated approach that assesses, builds and manages your cyber security capabilities but also has the ability to respond to incidents and crises. Private equity houses should assess their cyber risks and establish action plans to improve their security posture. A rounded approach should provide organisations with confidence: in your people, technology and connections, how you manage risk, set priorities and respond to an incident or during a crisis.

<table>
<thead>
<tr>
<th>Building confidence in your digital future</th>
<th>Confidence in your people</th>
<th>Technology cannot keep threats at bay. It only takes one bad click to open the door to threats. Make sure your people understand security and act securely.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidence in your technology</td>
<td></td>
<td>Technology underpins your business. In the digital age you cannot do without it, and as your business changes so should your technology. While embracing the new, understand the need to protect vital information and legacy technology against cyber threats.</td>
</tr>
<tr>
<td>Confidence in your connections</td>
<td></td>
<td>Organisations exist in an increasingly complex digital ecosystem. We are sharing information, and transacting digitally, more than ever before. You need to manage your exposure effectively so only those who should have your information do so and your information and transactions cannot be manipulated.</td>
</tr>
<tr>
<td>Confidence to take risks</td>
<td></td>
<td>Success in the digital age means understanding the opportunities it presents, while managing the inherent risks. Some risks are worth taking, but if you are struggling to manage the downside, you will not be able to take advantage of the upside.</td>
</tr>
<tr>
<td>Confidence during a crisis</td>
<td></td>
<td>Most organisations will be breached. Resilience means being able to react quickly and effectively when compromised. Being aware of and prepared for threats will help you prevent incidents and react to them quickly enough to reduce their impact.</td>
</tr>
<tr>
<td>Confidence in your priorities</td>
<td></td>
<td>Addressing cyber threats helps you prioritise what matters most. Being prepared for changes in the digital era will help you get your priorities straight. A ‘cyber savvy’ governance and management structure means you can prioritise opportunities and know where you can afford to take risks.</td>
</tr>
</tbody>
</table>
Ensure you, and your portfolio are not already compromised

According to the BIS 2014 Information Security Breaches Survey, 81% of large organisations and 60% of small organisations were compromised last year\(^1\). Although these figures were down from the year prior, it is still highly likely that organisations have experienced a breach, are currently under attack or at risk of a breach. Tactics are also more sophisticated so it is possible that a compromise is underway but it has not yet been detected. This is supported by reports that 75% of breaches take a cyber attacker a day or less to compromise an asset and only about 25% of those breaches are detected in the same timeframe.

In assessing its cyber risk it is imperative that organisations conduct a ‘compromise discovery’ exercise to ensure that they are not already compromised. After all, there is little point in investing in strengthening security posture if there is already a breach in the network with access to the security plans. A compromise discovery would involve monitoring the organisation’s network and machines for a short period of time to ensure that a cyber issue does not already exist. If there is an issue, appropriate actions to remediate this immediately is recommended.

Be ready to respond

Inevitably, most organisations will at some point suffer a cyber breach. The key is to ensure there is a structured yet pragmatic plan detailing what and how an organisation needs to respond to the cyber breach and who needs to be involved. This should include aspects such as: who internally is responsible for leading the breach response; who to call if external technical response support is required; what to do if the response needs to be conducted under legal privilege – how to tell and what to do; how to handle the PR side of a breach; if you have lost customer data for example, what is the communication plan to stakeholders; and what are the Information Commissioner Office implications as a result of loss of consumer data in one of your portfolio investments.

These are all aspects that need to be considered by private equity houses and their portfolio companies. There are some simple steps an organisation can take to ensure they are ready to respond, including developing an incident response plan that articulates how to respond to a breach and make sure that clear internal ownership is assigned. Organisations should also consider setting up a retainer with a specialist incident response services provider so that in the event of a crisis, help is at hand.

\(^*\)There are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again\(^2\)

Robert S. Mueller III, Director, FBI

---

1. 2014 Information Security Breaches Survey, Department for Business Innovation & Skills (BIS)
Conclusion

Without a doubt, advances in digital capabilities provide a wealth of opportunities for organisations to progress, operate more efficiently and ultimately grow. Embedding the right security to protect your digital assets, however, is fundamental. Unfortunately there is a strong likelihood that every organisation will be breached at some point. Having a contingency plan will help you deal with the worst possible scenarios more effectively and with minimum impact to your firm.

Cyber threat actors vary widely. From insiders behaving badly, competitors seeking an advantage, transnational criminal enterprises stealing for profit, political activists seeking to expose sensitive information to damage reputation, or terrorist organisations disrupting services: regardless of the motive, preparation is key. Cyber security risks need to be recognised, understood and led by governments and boards. In order to ensure economic prosperity and privacy, organisations need to tackle the issue head on.

Cyber security is a business-wide issue, not a technology one. It requires the whole organisation to pull together and protect its future and the wellbeing of those it interacts with. The nature of its structure and operations of private houses widens its reach and digital footprint, thus increasing its risks of cyber attacks – both directly and indirectly through its portfolio companies. Cyber security, however, should not and need not be feared. By taking a holistic view and focusing its efforts, all organisations, including private equity houses, can build confidence and resilience in their operations to help them protect what matters most, align priorities and make informed choices about their future investments.

Final thoughts for private equity houses

- Private equity houses are themselves a target for threat actors who may be looking to gain insight into a merger or acquisition for competitive advantage, or to obtain sensitive financial information.
- It is important that private equity houses understand the risks they face as a business and ensure that these risks are managed appropriately.

Final thoughts for portfolio managers

- Organisations that private equity houses are considering or have invested in are likely targets of cyber attacks.
- Cyber risks will vary across the portfolio depending on a number of factors, such as the amount and sensitivity of intellectual property, dealings with financial transactions, the volume of customer data, or the sector in which the organisation operates.
- A cyber breach may erode the value of an investment and impact potential exit plans. The risks to portfolio companies need to be considered at an individual organisation level.
About the Sponsor

PwC

PwC is among the leading professional services networks in the world. Our cyber security team, part of an international network, advises organisations large and small. We provide a range of integrated cyber security services with specialists offering risk assurance, forensic, legal, technology, and people and change consulting services designed to provide our clients with the confidence they seek. We are equipped to help organisations with detailed data and technical analysis, and equally, we can advise senior management and boards in shaping a broader strategic response to cyber risk. Our specialists help organisations reduce their exposure to cyber threats, improve their defences and respond to cyber incidents, as well as address the legal issues around breaches, data privacy and protection, and implement the requisite culture and environment where your people understand how to behave and do the right thing.

PwC offers a unique service offering where we bring together the breadth of capability that clients need to operate as an integrated team. We are globally recognised as a leader in cyber security. Internationally we were ranked #1 in Gartner’s Professional Security Consulting Services 2013 competitive landscape report, and praised by Forrester as a firm with strong global delivery capabilities with the ability to address the security and risk challenges our clients face.

With one of the largest dedicated forensic teams globally and over 100 UK-based cyber security specialists across risk, finance, legal, technology and people and change, PwC is the safe pair of hands, trusted by government and industry to handle some of their most sensitive issues. With offices in 157 countries, we are confident that our international network can provide our clients with local and global expertise and support they require.

Contacts

Kris McConkey
Partner, Cyber threat detection and response
kris.mcconkey@uk.pwc.com
+44 (0)772 570 7360

Richard Horne
Partner, Cyber security
richard.horne@uk.pwc.com
+44 (0)777 555 3373

Stewart Room
PwC Legal partner, Cyber security and data protection
stewart.room@pwclegal.co.uk
+44 (0)207 213 4306

James Rashleigh (Author)
Director, Cyber security
james.m.rashleigh@uk.pwc.com
+44 (0)780 802 8337