KPMG

BT

TAKING THE OFFENSIVE

Working together to disrupt digital crime

CONTENTS

FOREWORD

We live in a world where technology is all omnipresent. Every aspect of human activity – business, defense, healthcare, education, for example – is now reinforced by complex interconnected technologies and communications systems.

Those systems have never been more global. Information travels around the world in seconds, enabling businesses to run integrated supply chains, outsource operations and address international markets.

At the same time, we are clearly living through a period of rapidly increasing uncertainty and risk. This is no coincidence. Part of that risk stems directly from our dependence on digital technology.

Our dependency on technology raises significant governance issues with executives constantly having to balance questions of cost, risk and resilience. Today, digital security sits at the top of the boardroom agenda. Executives are all too aware of the risks, regularly discussing them with their colleagues.

Such discussions rarely bring comfort. As accredited organizations deploy more sophisticated technologies as a catalyst for improved performance, criminal organizations sense opportunity. Digital transformation has created new vulnerabilities that criminal groups are quick to exploit and monetize.

This is something BT and KPMG witness first hand. We see the challenges that CEOs and their boardroom colleagues face in staying informed of the changing face of digital crime, and we know that the sheer scale of digital criminality raises major questions about how to best manage risk and defend against a well-funded enemy whose strategies and technologies are constantly evolving.

New thinking is required, and the first step is to understand the digital criminal in terms of motive, method and how they intend to cash out. The next step is to turn that understanding into a cohesive and effective response.

> “NEW THINKING IS REQUIRED... TO UNDERSTAND THE DIGITAL CRIMINAL IN TERMS OF MOTIVE, METHOD AND HOW THEY INTEND TO CASH OUT.”

As the risk of digital crime grows, I believe businesses must be proactive. Rather than simply putting up defenses, organizations should recognize that all of us have a common interest in taking action to protect our data and that of our customers. The most effective way to do this is collaboration. By working with government, law enforcement, peers inside their sectors, organizations in other sectors and security specialists, businesses can make it harder and more costly for criminals to operate.

Security is not competitive. Digital crime is making it difficult for all businesses to fully exploit the new digital technologies that fuel growth and drive profit. By working together, we can turn the fight back on the criminal attackers.

Sir Michael Rake, Chairman,
BT Group Plc

EXECUTIVE SUMMARY

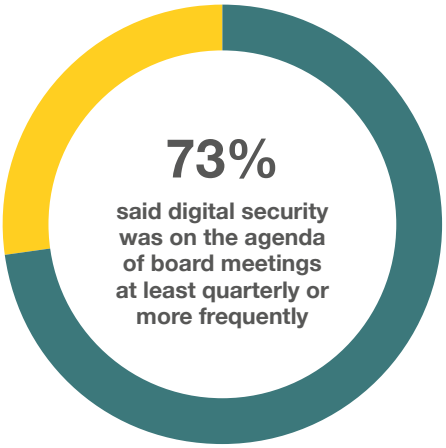
The world's biggest companies are facing an unprecedented number and variety of digital attacks by ruthless criminal entrepreneurs.

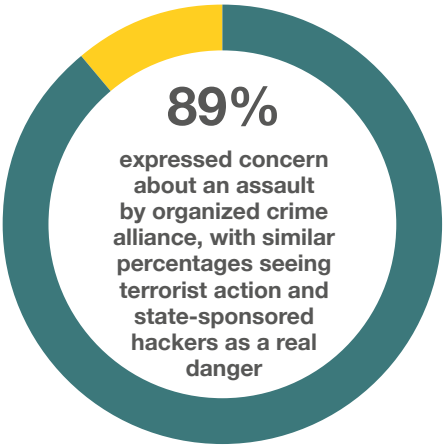
The scale of the threat and the tenacity of attackers shouldn't be a surprise. With the size of the internet economy alone estimated to be about $4.2 trillion in 2016 (Boston Consulting Group[1]) and online trade accounting for an ever-increasing share of global GDP, criminals inevitably see opportunities in the vulnerabilities of digital businesses.

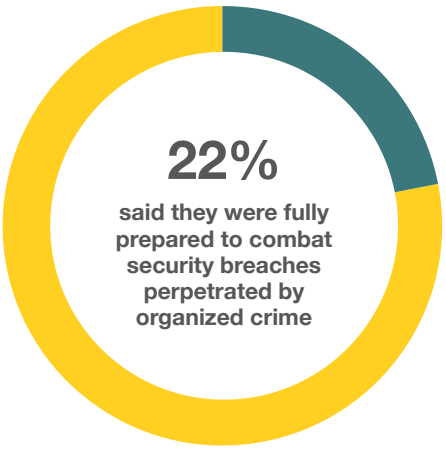
But although awareness of the threat has never been higher, a majority of businesses do not comprehend the methods and motivations of the attackers or fully understand the scale of the threat. Only a small minority feel fully prepared. Against a backdrop of proliferating attack tools and increased sophistication on the part of cyber criminals, businesses of all sizes are struggling to keep their data and systems secure.

Our findings and recommendations are drawn from interviews with clients and evidence gathered from work carried out by BT and KPMG. From the perspective of our ringside seat on developments in the digital world, we aim to identify the concerns of businesses as captured by a survey of organizations commissioned by us and carried out by an independent research agency.

As our research indicates, major organizations are committed to combating digital crime. We spoke to executives responsible for IT, resilience and business operations at major global companies, and 73 percent said cyber security was on the agenda of board meetings at least quarterly or more frequently. However, they face an uphill battle against enemies operating in a vast and dynamic dark market.







EXECUTIVE SUMMARY

A changing threat

This high level of awareness is clearly a good thing, and boards are increasingly educated about the nature of the threats they face and the range of potential attack strategies. Equally important, companies know the consequences in terms of customer confidence and share price.

However, few companies can confidently say they are doing enough to prevent attacks. When asked about measures to combat security breaches perpetrated by organized crime, only 22 percent of respondents said they were fully prepared.

Ruthless criminal entrepreneurs

Digital crime is driven by a vast criminal dark market. It is a marketplace in which attack tools are constantly developed and sold or hired to criminals, and it is supported by high levels of R&D spending. The methods used by the criminal entrepreneurs who operate in this market are constantly changing. Their agility makes it extremely difficult for legitimate businesses to keep pace.

The threat faced by businesses is constantly evolving. New methods of attack are created every day, and businesses are constantly dealing with unfamiliar tools and strategies.

The criminal entrepreneurs behind such attacks are ruthless but they also execute highly rational business models. Like legitimate entrepreneurs, their goal is to make a profit and they do this by monetizing their access to computer systems, networks and processed information.

The methods used extend beyond distributing malware, for instance. As the potential gain increases, organized crime groups are prepared to exploit and blackmail employees and deliberately place people on the inside.

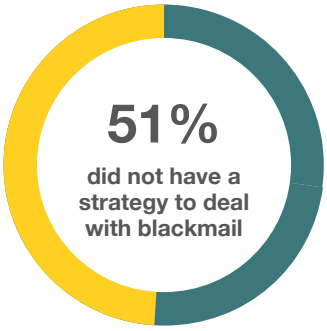
Fighting back

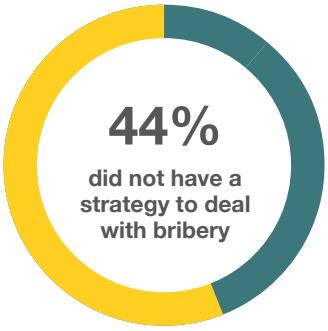
The threat posed by criminal entrepreneurs needs a proactive and immediate response. Companies must counter the activities of their attackers. This is often seen in terms of deploying additional security technology, employing more people and putting security policies and practices in place. But it is equally important to understand the attackers: Who are they? What are their business models? What is their goal? This knowledge can be used to create defense strategies that go beyond simply keeping intruders out of a network.

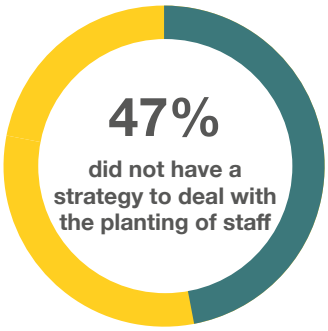
The need for agility

To counter criminal activity, businesses must be at least as agile and as flexible as the attackers, and there are clear challenges. How, for example, does an individual company compete with an organized crime group utilizing malware that is not only unfamiliar but also customized for a particular attack?

Collaboration provides a way forward. Organizations working in the same sector face similar threats and have a common interest in making it more difficult for criminals to operate. Extending that principle, banks, telecoms companies, Internet service providers (ISPs) and business in all sectors face a common enemy and in many cases an attack on, say, a retailer, might also involve a telco/ISP or bank. Equally, the goals of government and law enforcement align with the interests of commercial organizations in cracking down on illegal activity. By collaborating, businesses, government and law enforcement can share intelligence, resources and best practices and in doing so match the agility of criminal gangs.







Eyes on the prize: risk and opportunity

Robust digital security is not only vital for protection but is also an enabler. Security is the key to exploiting the potential of new digital channels to sell more goods and serve customers better. Equally, security is key when companies use digital to drive internal efficiencies; participants to our research see these as priorities.

Without robust security the potential to realize the benefits of digital technology is limited. The challenge is to exploit the opportunities and manage the risk. New thinking is needed.

The report will look at these themes in more detail, as we explore how businesses can take the fight to attackers. In a rapidly evolving landscape this will require a commitment to close collaboration with government, law enforcement and other businesses.

> “THE CHALLENGE IS TO EXPLOIT THE OPPORTUNITIES AND MANAGE THE RISK. NEW THINKING IS NEEDED.”

RETHINK THE DIGITAL SECURITY THREAT

01

THE DIGITAL CRIME GAP

Digital crime is rising at an astonishing rate, but while businesses are aware of the sharp increase in risk, that awareness has not translated into effective action. The vast majority of businesses have experienced some kind of attack but only a minority feel fully prepared to face the growing threat.

97% of companies have been the victim of digital attack and yet only **22%** are fully prepared to deal with incidents in the future.

55% have seen an increase in cyber attacks but only a minority – **23%** - have insurance cover in place to cover the cost of major incident.

71% have procedures in place to review the tools and strategies deployed by cyber criminals but few – just **30%** - understand them.

73% say digital security is on the board agenda, with **54%** having also educated their executives.

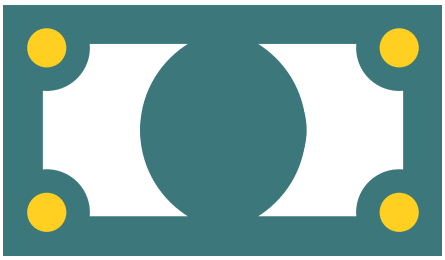
RETHINK THE DIGITAL SECURITY THREAT

01

No one doubts that an attack by digital criminals is a real and present danger, but the scale, rapid growth and ever-changing nature of the threat are often not fully comprehended.

According to research by the Centre for Strategic and International Studies (CSIS), and Intel Security, digital crime currently costs the world an estimated $400 billion every year[2]. This is beginning to matter, and risks are becoming a drag on the growth of our digital economy. Against a backdrop of extensive and constant criminal activity, conventional wisdom states that companies must be successful in defending their systems 100 percent of the time since digital criminals only need be lucky once to reap huge rewards. This is a huge challenge and is even beyond the capability of government. So it is now time to think beyond simply defending systems and focus on managing risk and being prepared to respond to and recover from attacks.

Digital crime currently costs the world an estimated



$400bn

each year

Digital criminality also exerts a high toll on individuals. The San Diego-based Center for Identity Theft Research estimates that 169 million personal records were breached worldwide last year.[3] This may just be the tip of the iceberg, as many of the security failures that allow such data to be accessed are not made public. This could change as governments demand greater transparency over data breaches. For instance, the European Union's General Data Protection regulation includes a mandatory disclosure requirement.

Prioritising digital crime

The scale of the problem has also been highlighted by governments and their agencies: for example, the UK National Crime Agency has made it clear that digital crime represents one of the most significant criminal threats facing Britain. As far back as 2010, the UK's National Security Council cited digital attacks among the highest-priority risks to national security.[4] In response, the UK government has announced a £1.9 billion investment to support a National Cyber Security Plan[5], which is likely to be spread over five years. Meanwhile, in the US this year, Securities and Exchange Commission chair Mary Jo White warned that digital crime was the "most pressing" threat to the financial system. The US government has been attempting to shore up its own defences. President Obama has presented a $19 billion budget spending plan[6] on security in 2017 compared to $14 billion in the previous year. Stepping back to look at the bigger picture, research organization Gartner estimated that spending on digital security in 2015 was at $75bn.[7]

An evolving threat

Every second, new malware is created and distributed and new phishing campaigns are launched. However, that doesn't mean that as new attack tools enter the frame the old ones vanish. Conficker, an early form of malware able to spread through networks, was launched back in 2008. Despite this, CERT-UK reported it was still the most prevalent malware in the UK.[8] A

helpful reminder that if left unpatched, legacy IT can still be a weak point in our digital defences. Malware authors are savvy—they exploit old systems but will also respond to security team activity by adapting their methods. Attack tools disappear and reappear again in an upgraded form – one that requires a new security response.

A case in point is Gameover Zeus, a malware used to steal usernames and passwords. Since being discovered in 2011, the software has been upgraded to include a distributed denial of service (DDoS) component, and refined to make detection much harder.

> "IT IS NOW TIME TO THINK BEYOND SIMPLY DEFENDING SYSTEMS."

As malware changes, so do the distribution tactics. Over the past few years, organizations and individuals have become increasingly aware that suspicious emails known as phishing may include attachments with malware embedded, but these can be hard to spot as criminals have become adept at sending messages that appear credible and relevant to the recipient. For instance, at the end of the 2015/16 tax year many UK taxpayers received emails claiming to offer advice from the tax authorities. This trend is also seen in the US as the tax-filing date approaches.

Phishing tactics are also constantly evolving and a new trend emerges towards an email compromise scam. This is often characterized as 'CEO fraud' or 'whaling'. Typically, employees receive apparently internal emails from senior executives often accompanied by spoof phone calls and text messages asking them to wire money to a named account or pay bills. In some cases, attackers will also hack the networks of professional advisers (such as lawyers) as part of these scams, allowing them to send emails that originate from a legitimate source. Organizations must constantly be on their guard.

And the amounts involved can be considerable. In one case, the financial controller of a healthcare company wired $18.5m to accounts in Hong Kong and Tunisia after receiving fraudulent instruction from someone posing as a senior executive.

Criminals are also using existing malware in new ways to support innovative criminal business models. For instance, criminals who deployed the Dridex malware – developed to harvest bank account details from target computers – have seen their major banks develop much more effective defenses. In response, the criminals have targeted firms which do not have such sophisticated defences in place. The criminals have also turned to Locky, a piece of so-called ransomware that encrypts files when downloaded onto a PC or network. The victims are unable to unlock those files until a ransom has been paid.

This rise in ransomware has been driven in part by the arrival of block chain currencies – notably bitcoins – that facilitate payment. The result is a twenty-first century variation on the age-old crime of extortion. Instead of thugs with baseball bats collecting cash, businesses are being robbed by criminals armed only with sophisticated attack tools and a knowledge of corporate vulnerability.

Criminals cast a wider net

The net cast by criminal entrepreneurs is widening. In the case of attackers who seek to profit directly from their efforts, early targets included banks (where account details could be used to clear accounts) or retailers (a source of credit card numbers, which could be used by the perpetrators or sold on). However, criminals have been more sophisticated and much more aware of the business models used by a wide range of firms. This allows them to develop new ways to target those business models. New security procedures have been matched by new tools developed by digital criminals. For instance, at a time when password authentication is increasingly augmented by a second factor – such as security questions – criminals have developed tools to harvest both pieces of information.

Take the insight from a key customer in the financial sector as a case in point: "There is increased awareness of how financial institutions operate and potential attackers have more information on the value chain. That means that institutions that were once difficult to monetize are now increasingly a target. Will Dixon, Deputy Director of Intelligence at Barclays, sees the criminals looking at softer targets: "We're seeing criminals increasingly targeting SME's and high value account holders."

Against this backdrop, security teams are struggling to keep up with the advances made by digital thieves. And that challenge extends beyond the 'four walls' of the organization itself. In a connected world of remote working, bring your own device and complex supply chains, businesses are being forced to take a much broader and more community-based view of how to manage their vulnerability to attack.

RETHINK THE DIGITAL SECURITY THREAT 01

So what we're seeing is a digital crime landscape that is constantly shifting not only in terms of rapidly evolving software attack tools but also the increased sophistication and agility of the tactics used by criminal gangs. And as the threat grows, the resources deployed by individual companies are increasingly dwarfed by the resources and talent available in the criminal dark market. Looking forward, businesses will have to rethink their digital security, and the first step is to understand the actors.

Rethink the Digital Security Threat – *Action points:*

- Gather intelligence on changing criminal tactics and new threats. Your employees and clients are often your best way of detecting attacks so ensure they know how they might be targeted. Include regular and concise updates on attacks in your internal communications and create channels to make it easier for employees and clients to raise issues and share information. Be an informed customer for cyber intelligence, demand actionable intelligence and look to your own security team to tailor it to your company's needs and business model.

- Think like a criminal. Working with your management team, identify the information and assets criminals would want to target and why.

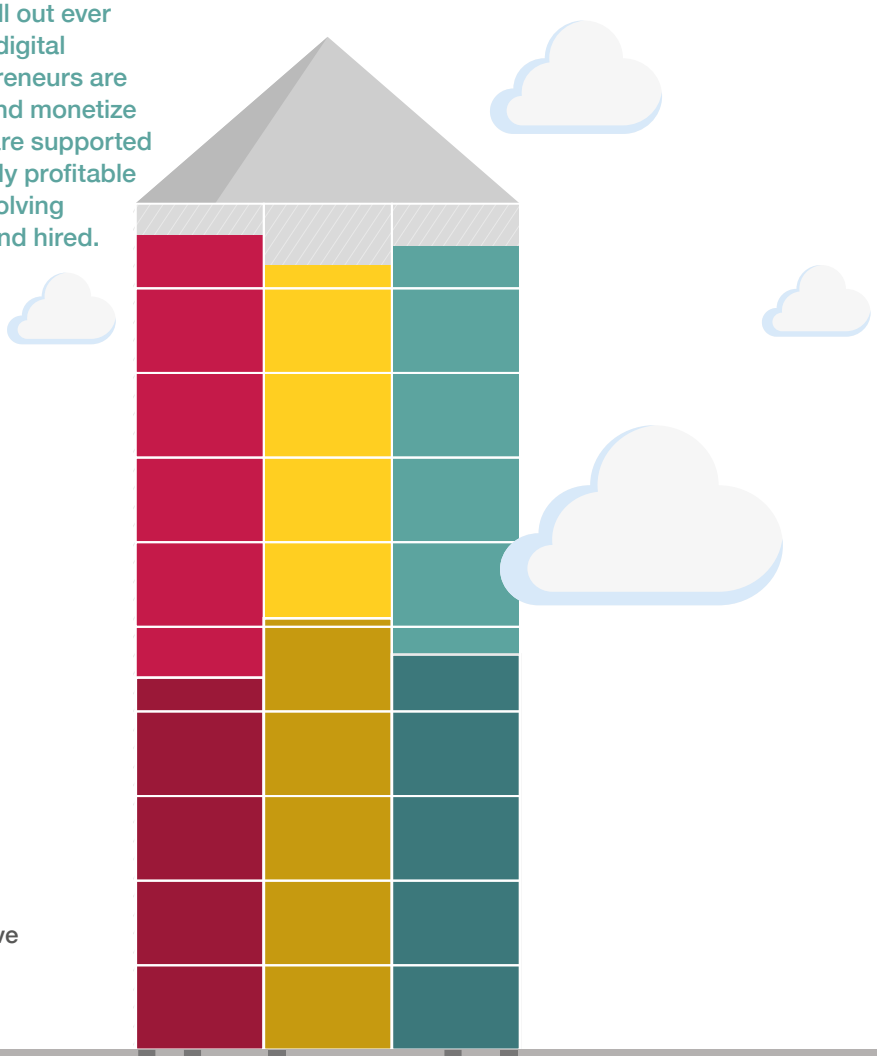
- Build out strategies to focus your investment on getting the basics right in terms of protecting your most sensitive information and being able to respond if it is compromised.

RUTHLESS AND RATIONAL ENTREPRENEURS

02

THE DIGITAL CRIME BUSINESS

We live in a world where technology is omnipresent, and as businesses roll out ever more sophisticated and ambitious digital strategies, ruthless criminal entrepreneurs are seizing the opportunity to exploit and monetize vulnerable systems. Their attacks are supported by a vast, well-resourced and hugely profitable dark market in which constantly evolving attack tools can be easily bought and hired.



96%

of businesses admit criminal entrepreneurs could be bribing employees but only **44%** have prevention measures in place.

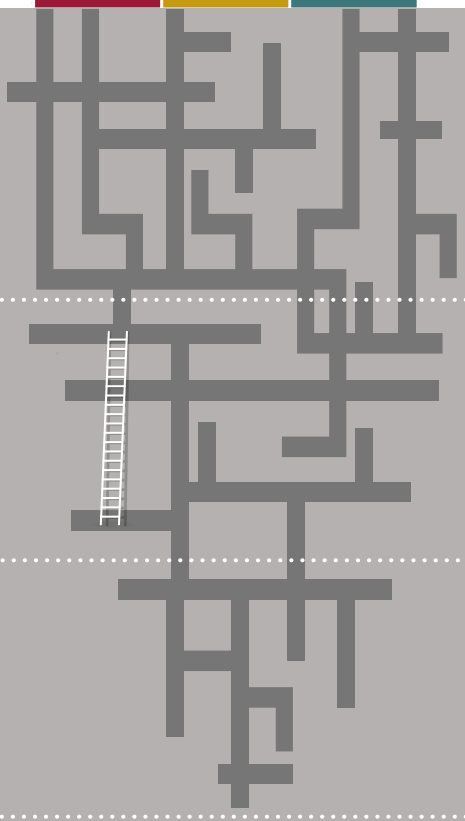
47%

47% do not have plans to counter the planting of people within their organizations, despite **94%** seeing it as a potential problem.

95%

say staff could be vulnerable to blackmail but less than half (**47%**) have a defence strategy.

CYBER UNDERWORLD



TIER 3
Commoditized attacks against everyone

Hundreds of millions of people attacked

100 Million x £1,000 = £100 Billion

TIER 2
Targeted attacks against businesses and wealthy individuals

Tens of thousands of people attacked

30,000 x £300,000 = £10 Billion

TIER 1
High end cyber attacks against financial systems

Tens of firms attacked

10 x £100 Million = £1 Billion

RUTHLESS AND RATIONAL ENTRE-PRENEURS

02

Business models

The twenty-first century digital criminal is best characterized as a ruthlessly efficient entrepreneur or CEO, operating in a highly developed and rapidly evolving dark market. Digital crime chiefs seek to make money by discreetly disrupting their target markets and exploiting the vulnerabilities and weaknesses of companies who honestly serve their customers. In short, they are a CEO without the constraints of regulation or morals, but who can face rather stiffer penalties if they fail to make money for their demanding shareholders.

To achieve their aims, they have developed a range of business models that allow them to cash out. Their technique may involve extortion by DDoS attack or ransomware, fraudulent manipulation of systems, or theft of data. They may use the data directly (for example, by clearing bank accounts), sell it onto other parties, or blackmail their victims.

Criminal entrepreneurship is not confined to those who directly attack organizations. The criminal who mounts a DDoS attack or who steals credit card details is supported by a vast dark market where attack tools are sold or hired – and crime is available as a service. Those who practice their trade within this dark market are entrepreneurs themselves with an eye on the bottom line. They will supply – sometimes for sale but often for rent – attacks tools. For a fee, they will conduct DDoS campaigns, distribute malware or build phishing websites. And for those who need the services of a hacker, they are available for hire to hack home networks and compromise the identity of the network owner.

And the compromise of home networks can not only damage the individual but also his or her business and possibly also a bigger marketplace. For instance, in one case a hacker broke into a CEO's account and used his identity to purchase shares. News of the purchase was then used to manipulate the market. In other words, what we're looking at is a dynamic and responsive market.

The three tiers of digital crime

There are three distinct tiers to digital crime, as defined by their targets. At the top level, criminals carry out high-end targeted assaults on the finance system such as the recent $81 million attack on the Bangladesh central bank, which but for the vigilance of other central banks might have been $951 million.[9] At the second tier, there are the regular attacks on businesses and high net worth individuals. And finally there are commoditized attacks affecting all of us. In each of these tiers, digital criminals map the costs and risks involved against the likely payout, just as any entrepreneur would.

89%

of attacks have a financial or espionage motive

At the commoditized end of dark market activity, campaigns target hundreds of millions of victims who stand to lose anything from $100 to $10,000, whether it is funds extracted from a bank account or a bitcoin payment extorted in response to a ransomware attack.

RUTHLESS AND RATIONAL ENTRE-PRENEURS

02

But the cost of mounting an attack is relatively low. Attack tools can be hired on a crime-as-a-service basis with no upfront costs. On a pay-per-use basis, it can cost as little as $0.50 to install malware on individual PCs, and a DDoS attack costs just $5 per hour[10] to mount but more than $40,000 an hour[11] to defend against. But it's not without risk for the criminal. These attacks are high profile and the security community responds quickly to block attacks. It's a game of cat and mouse. As attacks are identified, law enforcement steps in to prevent the criminal activity.

Attacks on businesses need a more custom approach. Again, the attack tools can be bought on a crime-as-a-service basis, but the criminals must also invest in the intelligence needed to understand their targets and monetize their vulnerabilities; tailored malware may also be required. The rewards are high – between $10,000 and $10 million – but criminals face stronger defenses. Patterns of fraud can be detected, although the victims can be publicity shy.

Those who target the finance system make a bigger investment in tailored malware and research, and perhaps also by placing people into target organizations. The criminals' investment in time and effort is large, but so are their returns. The cost to victims runs from between $10 million and $1 billion, and targets who fail to secure their systems also face fines from regulators.

This is the highest-risk area for criminals. Law enforcement has made attacks on the finance system a priority for high-profile takedowns, and criminals might find it hard to launder the money they've taken. Nevertheless, one successful campaign can deliver life-changing sums of money to the perpetrators, so the incentives are high.

Profits on a vast scale

Cases currently in the public arena highlight the scale of profits that can be made.

For instance, last year, Russian hacker Vladimir Drinkman pleaded guilty in a US court to stealing credit card details between 2005 and 2015, generating losses of $300 million. In the same year, Ivan Turchynov pleaded guilty to hacking newswires and using pre-release information to make illegal share trades. His operation generated revenues of $100 million.

> "A DISTRIBUTED DENIAL OF SERVICE ATTACK COSTS JUST $5 PER HOUR TO MOUNT YET MORE THAN $40,000 AN HOUR TO DEFEND AGAINST."

As the criminal threat is global, so is the response. In December 2015, an Interpol operation that took down call centres in China, Hong Kong, Korea and Vietnam involved law enforcement from more than 23 countries.[12] Fifteen call centres were taken down and 500 people arrested. This not only indicates the scale of the criminal operation but also the effort needed to take effective action.

It is important to remember that digital attacks are not carried out simply from malign intent and nor are they random: the attackers and entrepreneurs are entirely rational and profit-motivated. Indeed, according to research by Verizon, 89% of attacks have a financial or espionage motive.[13]

The ransomware arms race

Encryption is a vital security tool, protecting personal and corporate data from the prying eyes of intruders, but in the hands of criminals it can also be used as an attack weapon. Ransomware is currently used by criminal entrepreneurs to extort ransom payments from companies and individuals. Typically, this is achieved by infecting a computer with malware that encrypts files. Once the data has been rendered inaccessible, the victim receives a ransom demand.

The ransom will be paid in bitcoins, with the anonymity of the virtual currency allowing criminals to receive payment while minimising the danger of being caught. Payments of 0.5 to 1.0 bitcoin are common. With the value of bitcoins currently standing at around £450 or $640, these demands are low enough to encourage a rapid response from the victim but high enough (when scaled across a multitude of infected computers) to deliver a profit.

The best-known example of ransomware is Locky. When examined by BT, Locky was found to have polymorphic design, meaning that the appearance of the code changed with every update while its core function remained the same. Thus, with each new version Locky could carry on doing its work, and the code changes prevented detection by conventional anti-virus-based security tools. Security professionals reverse-engineered the malware to stop further infections and, for a time, this was successful. However, Locky was quickly adjusted and improved to sidestep these measures. As the Locky experience demonstrates, defending against new malware is an arms race where both sides play leapfrog to gain the upper hand.

Ruthless and rational entrepreneurs – *Action points:*

- View your business as the criminal would. Task your executives to consider the potential impact of cybercrime on your business - it isn't just a technical issue for the security team.
- In anticipation of more sophisticated attacks, create a closer working relationship between security and fraud control teams to detect and block patterns of cyber fraud. Consider what cross-functional forums and governance mechanisms exist within your organization that would facilitate better detection.
- Remember there is no absolute protection against cyber-attack. Breaches can and will happen and what matters is how you respond to common scenarios if they do occur. Plan and exercise for these scenarios, educating your team and streamlining your response processes.

TAKING THE FIGHT TO THE ATTACKER

03

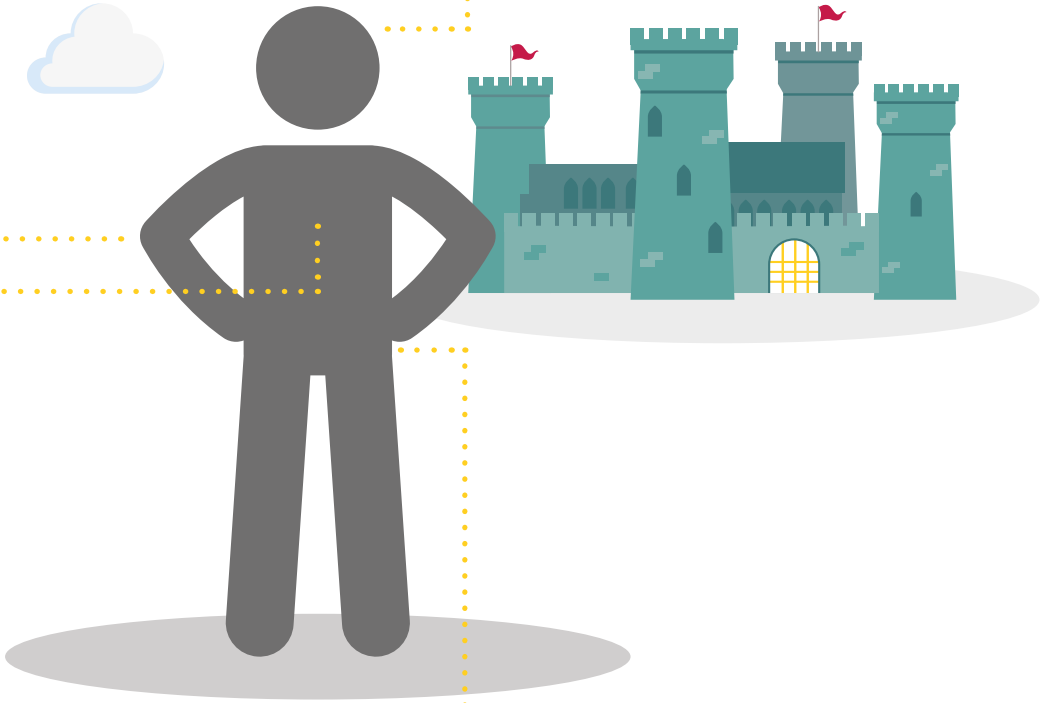
TAKING THE OFFENSIVE: MAKING CYBER ATTACK HARDER AND LESS PROFITABLE

The increasing sophistication and tenacity of cyber criminals mean that no organization can be 100% assured that its systems are secure. But businesses can take steps to make successful attacks more difficult, more costly and ultimately much less profitable.

1 Develop a multi-layered approach to security by making it harder for criminals to operate before, during and after an attempted or successful attack on a system.

2 Install and update all the tools required to minimize the likelihood of a successful attack.

But if criminals do break in, make it harder for them to achieve their goals. Protect information with encryption or deploy virtual machine technology to rebuild the system around them.



3 Make it harder for the criminal to cash out by deploying systems and procedures to limit the scope for using stolen data.

4 Build partnerships with peers, businesses in other sectors, telecoms companies, ISPs, law enforcement and government. Share intelligence and resources.

TAKING THE FIGHT TO THE ATTACKER 03

Organizations are struggling to keep pace with the efficiency of the dark market: every day of every year, new vulnerabilities are being identified and then exploited with breathtaking rapidity.

Witness the so-called Heartbleed bug, which allowed malign parties to read information in systems supposedly protected by the OpenSSL cryptographic software library. Digital criminals acted upon the vulnerability within 24 hours of it being disclosed.

However, that's only part of the story. Information on vulnerabilities is often traded on the dark market before it is publicly disclosed, allowing criminals to strike before businesses can prepare.

99%

of malware is used for under

1 minute

Businesses are also struggling to keep up with the attackers' ability to change their tactics to camouflage and conceal their activities. Malware infection is a case in point – 99% of malware is used for under one minute before the sample is changed to evade security software. Phishing emails are becoming more targeted, and change frequently as soon as they are blocked by security measures. This certainly isn't the epitome of sophistication – phishing emails are essentially the same kind of confidence tricks that would have been familiar to criminals 100 years ago. But they work, not least because the email messaging is regularly changed and carefully targeted.

"ORGANIZED CRIME IS DRIVEN BY A RETURN ON INVESTMENT," SAYS DIXON. " IT IS IMPORTANT TO PRESSURISE THE CRIMINAL CHAIN."

Law enforcement action

The prevention of digital crime sits high on the law enforcement agenda and both national and international-level police and other agencies have stepped up their actions. One manifestation of this is concerted efforts by Interpol, Europol and the FBI to take down bot nets – networks of infected computers that are used to send spam emails, distribute more malware or launch DDoS attacks. In 2014 and 2015, Europol took down four major bot networks, namely Gameover Zeus, Ramnit, Beebone and Shylock. This kind of activity has undoubtedly impacted organized crime groups.

A temporary solution?

Despite these successes, action against a particular attack tool may only take it out of the game temporarily. Law enforcement disrupted the widely used banking-sector attack tool Dridex in 2015, but it was operational again within three months. The wider point is that, within the dark market,

software and campaigning strategies are constantly refined. Successful action to disrupt a piece of malware might only buy time before it reappears.

What's more, criminal entrepreneurs tend to bounce back stronger and harder. "Botnet takedowns are hardening crime groups who are improving security and developing new methods," says Will Dixon of Barclays.

There is a danger that, although law enforcement and individual organizations fight today's battles, they will fail to see the new threats beyond the horizon. If today's business model is stealing bank account information from individuals and companies, tomorrow's might be the deployment of ransomware – such as Locky – to blackmail targets.

Hitting the attacker's bottom line

Rather than simply responding to events, there is a need to take the fight to the attacker. An offensive rather than defensive approach to targeting crime is increasingly being undertaken by law enforcement who have the legal powers to disrupt the technologies used by attackers and bring down money laundering operations. Businesses must also play their part by being more proactive in deploying security tools, procedures and strategies that make it more difficult and costly for criminals to operate. Including, increased co-operation with law enforcement to make it tougher for criminals to not only breach systems, but also use the information they steal and ultimately cash out. Working together, there is an opportunity to hit the bottom line of the attacker.

This requires a multi-stranded approach. The first line of defence is to keep criminals out of information systems. However, assuming that breaches do occur, organizations should make it much more difficult for the attacker to use the information.

For example:

- Detecting and ejecting intruders quickly.
- Restoring systems to a pristine state – for example using virtual machine technology.
- Protecting and limiting access to data using encryption.
- Putting in place additional security around the most sensitive systems.

If information is stolen, organizations should make it harder for the criminal to exploit it. Banks have led the way on this: thanks to a combination of chip and pin technologies and constant fraud monitoring to detect unusual activity, it is now much harder to use stolen credit card data.

Finally, once criminals have made a profit, they often can't simply spend the money. There is therefore an opportunity to close operations at the money-laundering stage. This will be a focus for Britain's National Cyber Crime Unit. Elsewhere in the world, law enforcement has its sights on illegal currency transfer and processing operations. For instance, in 2013, the FBI closed Liberty Reserve, with the authorities saying it had become the "bank of choice" for a broad range of conventional and digital criminals.

To take the fight to a well-resourced and sophisticated enemy, sustained by a dark market that develops attack tools and strategies more effectively than legitimate organizations build defences, we must develop a streamlined and coordinated approach that sees businesses working together with law enforcement.

"Any effective crime prevention strategy needs to combine good protective security with a robust deterrent approach: we've got to increase the real and perceived risk to criminals that, by attacking our business and our fellow citizens, they will get caught and punished", says Dr Jamie Saunders, Director of the UK National Cyber Crime Unit.

Taking the fight to the attacker – *Action points:*

- Build partnerships with law enforcement – this will ensure that if the worst happens you have the trusted contacts you need to respond quickly. This might mean creating the headroom for your team to participate in forums designed to respond to managed cybercrime.
- Share information with your peers. Cybercrime isn't a competitive issue – it hurts the whole community and you are all being targeted. Online and physical forums exist to allow this to happen in a trusted and confidential environment. Identify and join the most relevant of those forums.
- Look at how you can limit the ability of criminals to exploit your data if they are successful in stealing it. Ask yourself if you can detect and block misuse, or respond quickly to a breach? In answering these questions, model the most likely scenarios that could lead to exploitation of data. Foster collaboration with outside organizations (banks, law enforcement agencies, suppliers) who may be the recipients of attempts to exploit the data.

THE NEED FOR SPEED

04

THE DRAG FACTORS

Digital attacks can be carried out at breath-taking speed using tools and strategies that are constantly updated. Businesses must be as agile and quick on their feet as their criminal attacker but their response is hampered by a range of institutional, regulatory and technological drag factors.

49%
of the businesses we spoke to said they were constrained by regulation

45%
lacked skills and people

46%
were held back by a reliance on legacy systems

38%
cited inflexible processes within their organizations

94%
named reliance on third parties as a problem

THE NEED FOR SPEED 04

All businesses understand the importance of rapid action but, as our research indicates, obstacles stand in the way of a quick response.

Indeed, only 9% said they faced no hurdles to response.

When we asked senior decision makers within organizations what was hampering their efforts to respond quickly to the digital security threat, almost half (49%) said they were constrained by regulation, and 45% said they lacked the right skills and people. Other constraints were embedded in their organizations; for instance, 46% cited legacy IT systems as an issue, and 38% pointed to inflexible processes. A dependence on third-party providers and contracts with third parties were also seen as issues, as was a resistance to cultural change and lack of investment.

In the broadest sense, it's clear that even before you look at the problem of matching dark market R&D, there are many obstacles to a dynamic approach to digital security. And that raises questions:

- Are regulatory regimes making it harder, rather than easier, for organizations to respond to digital threats?
- Is an increased focus on compliance hindering responsiveness and creating a culture of inflexibility within organizations?
- Are businesses too dependent on third parties to meet their security needs?

On that last point, our research found that a majority of firms have mostly or fully outsourced the running of their security, the investigation of incidents, the coordination of the organization's response and other major functions. The question then becomes, just what skills and capability have they retained in-house, and does their outsourced provider really understand their client's business sufficiently to provide a credible response?

Meanwhile, asked about what they expect from their in-house security teams, responsiveness, agility and trust topped the list of important attributes.

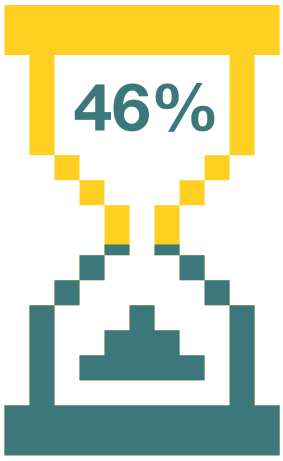
Solving the conundrum

Organizations know their security teams must be both responsive and agile to combat the growing threat. But, at the same time, they feel the effectiveness of their defence is constrained by a range of factors, including a reliance on third parties to which much of their security has been outsourced.

The way forward is to build an approach to security that recognizes and responds to the changing threat. This will involve a commitment to threat and vulnerability management, coupled with the capacity to upgrade defences as new threats emerge – and this is constantly. To stay ahead of the game, businesses need an effective digital/threat intelligence capability. The organization needs to be able to spot new trends and threats with a view to making sure that it can respond.

Building a digital threat intelligence capability is about much more than collating technical information on the systems used to launch attacks. Companies need to gather evidence-based information on potential attackers, the tools they use, their motivation and the vulnerabilities they exploit. By sharing data, businesses can improve their own security and cut intelligence-gathering costs. All of this should be seen not only in the context of present but also future threat. Crucially, intelligence, if it is to be effective, must be actionable and acted upon.

When we asked CEOs what was hampering their efforts to respond quickly



cited legacy IT Systems as an issue

As a key customer from the finance sector stresses the importance of threat intelligence but warns that it is not always used. "There is a parallel with business intelligence," he says.

Common patterns of attack shouldn't be ignored: businesses should have the tools and processes in place to deal with known dangers. There is also scope to redesign the way that systems are built.

And, as Robert Coles, Chief Information Security Officer at pharmaceuticals business GSK, points out, the human factor – in terms of security culture – within organizations shouldn't be ignored. "We are very interested in the human dimension and the importance of awareness-raising and education within organizations and driving cultural change," he says, adding that collaborative work is underway with Royal Holloway University on how to influence security culture.

Sourcing expertise

At a time when the threat of digital crime is constantly changing, businesses should also have an understanding of where they can rapidly source expertise that isn't currently available, either in-house or via a third-party security provider. There is a role not only for the digital security industry but also for government agencies and the developing cyber insurance sector.

Our research, coupled with our widespread experience of working with clients, suggests that boards expect insurance companies primarily to provide compensation to clients or customers. A majority of companies also see the role of insurers as covering liabilities, covering direct financial loss and providing identity fraud protection.

However, there is also a strong case for working more closely with insurance companies to prevent digital crime. One service the industry could provide is putting companies in touch with third-party experts in key aspects of security.

Collaboration

There is a need for collaboration between law enforcement agencies and businesses. To take an example, law enforcement has legal powers to disrupt the infrastructure used by criminals but it doesn't always have the resources. Companies could fund the development of tools and campaigns that can be prosecuted by law enforcement.

> "COMPANIES COLLECT IT BUT OFTEN THE DECISIONS ARE MADE ON GUT INSTINCT. I AM A BELIEVER IN THREAT INTELLIGENCE BUT IT IS ONLY USEFUL IF ACTED UPON."

There are restraints; for instance, certain agencies are prohibited from receiving funding. As Robert Coles of GSK says: "Industry can cooperate with law enforcement but legally there are limits on what we can do. The emphasis should be on pooling information with law enforcement."

THE NEED FOR SPEED

04

The scope for collaboration extends beyond contact between individual businesses and law enforcement. Citing his own sector, Will Dixon of Barclays says: "It is important to develop operational partnerships between finance, telecoms, ISPs and government to create an operational framework for cooperation. The NCSC [National Cyber Security Centre] can play a key role in this."

Although there is huge scope for businesses operating in the same or similar sectors to share information on common threats, cross-sector collaboration between, say, banks, telecoms companies and retailers can also be crucial in preventing criminal activity. For instance, one way that criminals breach bank security is to convince telecoms providers that a phone has been stolen and when the telco transfers the number to a new SIM card, the thieves use an activated device to reset the passwords of the legitimate owner's online banking or intercept two factor authentication messages. By sharing intelligence, banks and telecoms owners are much better positioned to combat this type of fraud or intercept two factor authentication messages.

Sharing information can also help save organizations money, reducing the need to buy in information from security companies.

There is an equally strong case for companies to fund innovation through accelerators and incubators. A case in point is Cylon (Cyber London) lab. Backed by government and private-sector funding, it is a London-based incubator established to provide security start-ups with support to develop their products and services to the markets. By working with, or funding, security-focused incubators and accelerators, corporates have the opportunity to support innovative R&D.

And security is an important component in the UK's wider technology start-up ecosystem, with the area around the Malvern Hills seen as an important cluster for established and new businesses alike. The challenge for organizations is to tap into this innovation and it is important to be proactive. This could mean allocating responsibility to senior security personnel to identify innovation. "I have a director of Digital Innovation," says Will Dixon of Barclays. "His role is to spot and respond to innovative new technologies."

The need for speed – *Action points:*

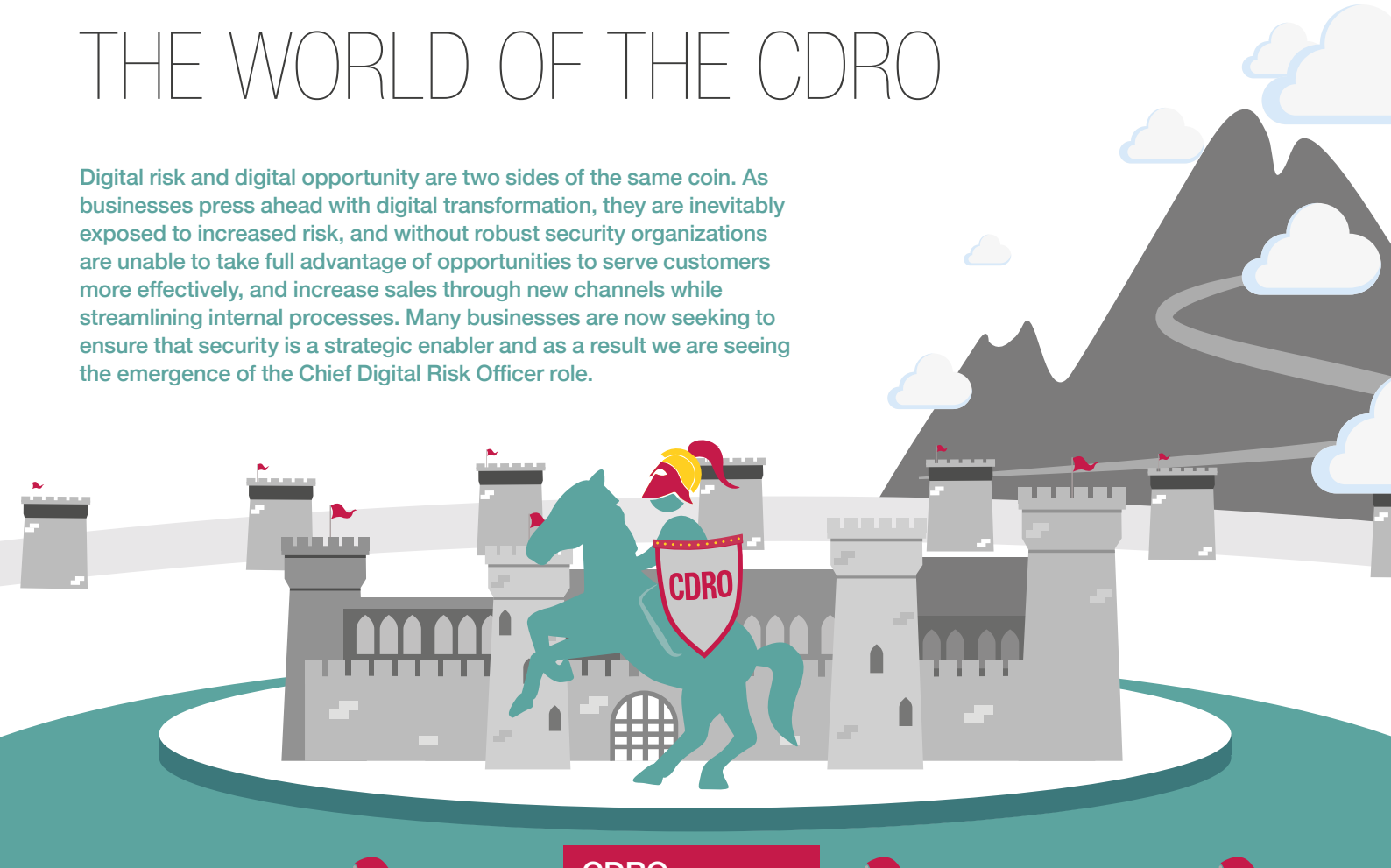
- Demand evidence that your cyber security team are able to respond quickly and flexibly to changing threats and give them the license and the support they need to do so.
- Work with your major clients and third parties to exercise a major incident. You will need their co-operation if you are attacked and working closely in this way builds trust and transparency.
- Prepare for the worst case – exercise your response to a cyber-attack and make sure you develop "muscle memory". This will help you to respond quickly by understanding how an incident might unfold and how you might respond.
- Consider the role of cyber insurance in helping you mitigate the financial impact and access specialist expertise when needed. You won't have all the skills you need in-house.

RISK AND OPPORTUNITY

05

THE WORLD OF THE CDRO

Digital risk and digital opportunity are two sides of the same coin. As businesses press ahead with digital transformation, they are inevitably exposed to increased risk, and without robust security organizations are unable to take full advantage of opportunities to serve customers more effectively, and increase sales through new channels while streamlining internal processes. Many businesses are now seeking to ensure that security is a strategic enabler and as a result we are seeing the emergence of the Chief Digital Risk Officer role.



CDRO Accountabilities

1 Digital Risk Innovation

- Monitoring of Innovation & Leveraging it
- Embedded Digital Crime Short-circuits in new Products

2 Digital Risk Identification

- First Line and Second Line Data Correlation
- Internal & External Loss Data Analysis
- Business Process Mapping
- Scenario Analysis
- Quantified Measurement & Comparative Analysis

3 Digital Risk Protection

Monitoring & Reporting:

- Digital Hygiene Implementation
- Digital Risk Analytics

Control & Mitigation:

- Digital Stress Tests
- Validation of Risk Transfer Options
- Capital Allocation

4 Digital Crime Detection

- Real Time Digital Risk Intelligence Sharing
- Dynamic Risk Profile Evolution
- Deep Learning Notifications

5 Digital Risk Response

- Automated Response via Orchestration
- Containment Strategies: Limiting the Blast Radius
- Offensive Strategies: Digital Crime Hunting
- Digital Risk Financial & Regulatory Disclosures

6 Digital Crime Recovery

- Digital Business Resiliency & Continuity

RISK AND OPPORTUNITY 05

The reward for effective security extends beyond stopping damaging systems breaches. Digital risk and opportunity represent two sides of the same coin. Since the arrival of internet-driven e-commerce in the mid-1990s, businesses have taken advantage of new channels and platforms – including PCs, mobiles and tablets – to sell more products and provide better service to customers.

Behind the scenes, businesses have also been improving their internal processes, cutting costs as they do. These innovations represent huge prizes but they also come with risk. Indeed, a business extending a basic e-commerce offering – to include not only mobile platforms but also network-driven omni-channel strategies, such as click and collect – is, almost by definition, also creating new points in the value chain where criminals can operate.

At one level, a commitment to robust security delivers a competitive advantage. As Will Dixon of Barclays points out, trust is one of the factors that underpins brand strength, not least in the banking sector. A demonstrably proactive approach to security underpins that trust. For its part, Barclays has made security part of its offering to customers by publicising the issue through its Digital Eagles scheme. The bank also offers free security software to customers.

The question of trust operates on a number of levels. At its most fundamental level, a customer's trust in the security of a system is a prerequisite for pressing ahead with a transaction. Most people will not commit information to a website, unless convinced the information is secure. But at a deeper level, trust is a key factor in maintaining brand strength and retaining customer loyalty. And loyalty can evaporate quickly. A major breach in security is often followed by an exodus of customers.

More importantly, in today's trading environment there are very few sales, customer service or back-office innovations that don't involve networks. Security is the catalyst for innovation; it frees companies to press ahead with new ideas and new channels.

User experience

The challenge here is that the balance between opportunity and protection against risk can be difficult to strike. Think for a moment about the customer experience on a typical consumer-facing retail website. Banks and retailers alike want to cut down on card fraud and one effective way to do this is to ask customers to key in a password registered with the card issuer before a transaction can be completed.

> "BALANCE HAS TO BE STRUCK BETWEEN USER EXPERIENCE AND SECURITY."

The problem is that such systems are hurdles to completion. Many customers faced with a request for a password will bail out and leave an abandoned shopping cart. Thus a balance has to be struck between user experience and security.

RISK AND OPPORTUNITY

05

More emphasis on security

The businesses we spoke to were keen to exploit the benefits: 92% saw digital as a means to create opportunities; 89% were keen to drive efficiencies; and 83% cited better customer service as a goal.

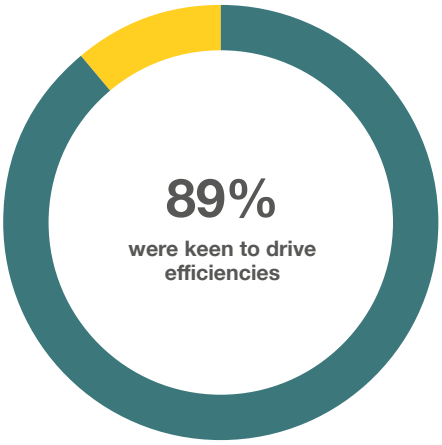
At the same time, respondents acknowledged that the pursuit of opportunity would place new demands on security chiefs. 70% of those interviewed wanted more emphasis on digital security, and 62% expected an increased focus on the mobile arena. Equally important, almost half said they wanted security chiefs to play a much more strategic role.

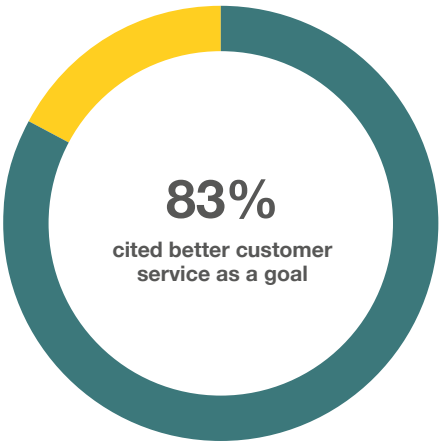
The Chief Digital Risk Officer

But what does that mean in practice?

One trend in recent years has been the appointment of Chief Digital Officers, often to oversee the transition to digital by traditionally analogue businesses. By its nature, this is a strategic role combining digital expertise with high-level management skills. In parallel, the Chief Information Security Officer takes responsibility for security.

What we're seeing now – and this reflects responses from those taking part in our qualitative survey – is a redefining of the digital roles. Some companies are appointing Chief Digital Risk Officers (or at least expecting their CISO to step up) to take responsibility not only for security per-se but also the development of policies and practices that allow organizations to develop new channels alongside innovative ways to deliver services to customers, and streamlined





back-office systems.

We expect this to emerge as a multifaceted role. Certainly CDROs will need a full understanding of all the issues surrounding threat prevention and detection and incident management. But the CDRO will also be in the enablement business, with security as a key component in helping companies sell more and improve performance. In addition, the CDRO will have a hand in functions such as governance, the development of risk management policies, compliance and auditing. However, the key is avoiding a compliance focused box ticking job, and focusing on enabling opportunity and demonstrating agility.

Risk and opportunity – *Action points:*

- Security is about balancing opportunity and risk. Build security into your digital strategy and the development of new channels. This can help your customer experience if you get it right. Think about how your organization uses cyber security to offer a trusted service to your customers while enabling new ways of engaging. Consider how you communicate your commitment to security externally.

- Remember digital security isn't a technical issue. It is part of doing business in our networked world and needs to be part of your wider strategic planning process – not just a stovepiped role. Ask if digital security is an integrated workstream in your business' annual and strategic planning processes?

- Consider putting a very different style of security chief – the Chief Digital Risk Officer – at the heart of your digital strategy.

CONCLUSION

The fight against digital crime does not have to be a losing battle but to be successful against a resourceful, well-funded and determined enemy, businesses must change the way they approach digital security.

To be simply defensive – putting up security barriers to keep criminals out of systems – is not enough. Instead, businesses should plan to be proactive: rather than responding to attacks, they should be taking action to counter the activities of the criminals. However, that doesn't equate to maverick action on the part of private sector businesses: activities such as taking down bot nets or disrupting money laundering operations are the province of law enforcement agencies.

> "BUSINESSES IN ALL SECTORS HAVE A COMMON AND ALIGNED INTEREST IN FIGHTING DIGITAL CRIME."

What all businesses can – and should – do is collaborate with their peers and work closely with law enforcement. They need to work with telecoms companies, ISPs, banks, credit card providers, insurers and the security industry in a concerted effort to make it harder and more costly for criminals to pursue their objectives. Businesses in all sectors have a common and aligned interest in fighting digital crime. By working together, they can exchange intelligence, fund innovation, share best practices and develop common strategies.

Businesses should also foster collaboration internally between departments and functions – for instance by ensuring that security and anti-fraud teams work together to facilitate criminal activity at every step, from system breaches to the point where attackers seek to monetize their activities by using or selling stolen data. It's important to remember that no system can ever be 100% secure, so a holistic, organization-wide approach is required.

As you develop security strategies, it's important to try and think the way your attacker thinks. Be proactive and demand and gather actionable intelligence, understand the motives of the attackers, map the changing trends in digital crime and use this information not only to equip and instruct your security teams, but also to mobilize awareness in the wider workspace. Introduce a culture that sees security not as a matter of compliance but as an ongoing process of identifying, assessing and effectively responding to new threats.

The prize is a better business. Security is the enabler that facilitates digital innovation and ultimately drives profit. The way forward lies in ensuring that security is central to delivering the strategic goals of the company. That takes us way beyond putting up fences. The successful company of tomorrow will understand the enemy and collaborate with partners to frustrate the attacker at every step, from breaching a system through to cashing in. The prize is reduced risk and improved performance.

REFERENCE

1. https://www.bcg.com/documents/file100409.pdf

2. http://www.mcafee.com/uk/resources/reports/rp-economic-impact-digitalcrime2.pdf

3. http://blog.trendmicro.com/the-most-prominent-cyber-threats-faced-by-high-target-industries/

4. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf

5. https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security

6. http://fortune.com/2016/02/09/obama-budget-cybersecurity/

7. http://www.gartner.com/newsroom/id/3135617

8. https://www.cert.gov.uk/wp-content/uploads/2015/05/Annual-Report-including-4th-Quarter-FINAL.pdf

9. http://www.nytimes.com/2016/05/01/business/dealbook/hackers-81-million-sneak-attack-on-world-banking.html?_r=0

10. The $5 figure is the typical cost of DDoS attacks by the hour from various black market surveys

11. The $40,000 figure comes from an Incapsula DDoS mitigation study from November 2014 https://www.incapsula.com/blog/DDoS-impact-cost-of-DDoS-attack.html

12. http://www.interpol.int/News-and-media/News/2015/N2015-223

13. http://www.verizonenterprise.com/verizon-insights-lab/dbir/

OLIVER for KPMG | OM061217A | June 2016