Making cybercrime prevention the highest priority

Matt Eddolls, CoreStream

The threat of cybercrime continues to evolve and grow as criminals adapt to new security measures and take advantage of changes to our online behaviour. The only constant appears to be our vulnerability: whatever new steps are taken by companies or individuals, the criminals always seem to be one step ahead.

The problem is that it isn’t an even contest. Hacking and online fraud is hugely profitable for organised crime, encouraging constant innovation and changes in attacks. A notable recent development has been the packaging of sophisticated malware tools into kits that require few specialist skills to use. Now, criminals at the top of the chain can simply license their tools in return for a cut of the proceeds. With hacked personal data now cheap and plentiful in online marketplaces, cyber-criminals have proliferated.

“Vulnerabilities can be exploited by cyber-criminals for months or even years before they are detected”

The nature of the Internet means that this crime knows no borders: criminal activity can be focused on the easiest and richest pickings and the perpetrators can be spread across the globe. Crime-fighting agencies have been overwhelmed by the volume of activity and stymied by the fact that so much of it originates from multiple overseas jurisdictions.

Huge flaws

The phenomenal success of Internet-based software and services over the past two decades has masked the fact that there are huge numbers of security flaws, even in well-established technologies. The recently exposed weakness in Secure Sockets Layer (SSL) to so-called DROWN attacks, which affected an estimated 33% of all HTTPS servers, is a classic example. SSL is the de facto encryption standard for secure connections and consumers have been told for years to ‘make sure the address is HTTPS if you want to be secure’. It’s a simple rule, it’s easy to check, and now it turns out that it isn’t true. Vulnerabilities like this can be exploited by cyber-criminals for months or even years before they are detected.

Having said this, technical flaws are no longer the problem they were. A decade ago, many companies were wide open to cyber-attack, thanks to poorly designed software and badly configured networks. As security awareness has increased, a large proportion of these issues has been fixed and finding and exploiting weaknesses has become more expensive and difficult for the hackers. As a result, they have switched to targeting people instead and this has proved far easier for them to do and much harder for us to prevent.

One significant problem is that computer users continue to be caught out by links to bogus sites and malware, despite being well-informed of the dangers. This is because phishing attacks have become increasingly sophisticated, refined by the criminals’ experience of what works. Victims are now socially engineered: specifically targeted and cleverly cultivated using bits of personal information picked up from many sources all over the world.
the web, including data stolen in breaches elsewhere. If the criminals have gained access to personal emails or customer account details, they can mimic the style and content of familiar communications to be all the more persuasive.

“Cracking passwords is often pretty straightforward for a hacker armed with the right software tools and a few personal details from social media”

Pervasive password reuse is another people problem. The average Internet user in the UK now has well over 100 accounts, each requiring an ID and password. It’s impossible to remember that number of separate login credentials, so many people devise a single obscure password and then reuse it everywhere – including their employer’s network – in the belief that it can’t possibly be guessed. In fact, cracking passwords is often pretty straightforward for a hacker armed with the right software tools and a few personal details from social media. More importantly, it’s increasingly likely that the password will be stolen in a data breach at one of the many organisations it has been used for. For organisations, this is a security nightmare; network security is reduced to that of the least secure system their staff have had dealings with.

Mobile problems

The widespread adoption of mobile and devices also brings problems, since staff use them in the workplace without properly considering security. This ‘shadow IT’ can be a major vulnerability, especially for smaller firms: they often don’t have the policies to govern it or the resources to manage it and their staff may be accustomed to adopting new technologies and adapting their work practices in order to get the job done more quickly and efficiently. This cavalier attitude belongs to a time when cybercrime was less of a threat and small businesses were less of a target.

In 2015, 25% of large firms and around 15% of smaller ones reported network penetration by unauthorised outsiders, while 90% of large firms experienced a security breach of some sort (the median number of breaches was 14). These relate only to detected incidents; the real numbers are probably much higher. Many companies are turning to cyber-insurance as a means of mitigating the risks of breach, but it is often difficult to define exactly where the blame lies and thus whether a breach is covered. In any case, insurance does little to arrest the growth of cybercrime, it simply shifts the costs elsewhere.

The EU’s forthcoming General Data Protection Regulation (GDPR) is unlikely to do much to reduce cybercrime, either. The GDPR extends responsibility for protecting personal data to almost any business that holds it, no matter what its size, including hosted service providers. It may lead to breaches and hacks becoming bigger news, due to increased notification to the Information Commissioner’s Office (ICO) and larger fines to the guilty parties. Organisations will probably put more resources into security and breach prevention as a result. However, the increased expenditure will probably only divert criminal activities towards softer targets.

Virtual arms race

New technologies and services, such as advanced encryption, two-factor authentication and password managers, will improve the defence against current threats. However, once their use becomes widespread, cyber-criminals are likely to repeat the patterns of the past and shift their focus to other – as yet unidentified – vulnerabilities. This is a virtual arms race and at the moment we’re fighting it badly.

“To get ahead of the criminals we need to change the way we do things. Everyone should understand that cybercrime is a threat to all organisations, whatever their size or type”

Cybercrime has grown enormously and will continue to grow because it is a relatively easy and safe way of stealing other people’s assets. The only effective way to reduce it in the long term is to attack it at source. The serious, organised, multinational element of the crime requires high-level international co-operation. Smaller-scale fraud has to be properly dealt with by the police and the criminal justice system, which may need to be better resourced in order to do so. Finally, perhaps those companies carrying and hosting the resources and traffic that make cybercrime possible need to be held to greater account.

In the meantime, to get ahead of the criminals, we need to change the way we do things. Everyone should understand that cybercrime is a threat to all organi-
sions, whatever their size or type. It will continue to grow and nothing that the Government or the regulators are doing at the moment is likely to curtail it. Therefore, it is up to business leaders to recognise the threat and to ensure that their organisations are adequately prepared and protected.

Unfortunately, according to current reports, only 37% of companies have any kind of cyber-incident response plan, and fewer than 50% of company board members have ever requested information about their organisation’s cyber-readiness. Astonishingly, as of 2015, 32% of organisations had not conducted any form of security risk assessment at all, according to the UK Government’s ‘2015 Information Security Breaches Survey’. This suggests a serious lack of risk awareness and good governance in far too many firms.

Technology has become integral to most business operations and almost all of that technology is networked. This means that cyber-criminals can gain access to sensitive data or intellectual property via almost any part of the business. Lost data can be replicated and distributed at will, so a breach can never be truly resolved and serious data losses may even threaten business viability. This makes cybercrime a serious strategic risk and plans for prevention and mitigation deserve the highest priority. However, many business leaders are content to leave cyber-security to the IT department, in the belief that technology can fix the problem. This is a dereliction of their duty to shareholders and reflects a fundamental misunderstanding of the threat, which is primarily linked to user behaviour.

Risk management

The process of risk management should be the same as for any other threat. The first step is to understand what makes the organisation an attractive target to cyber-criminals, and where the main vulnerabilities lie. Tackle these by breaking them down into appropriate tasks and responsibilities, assign those to the right people, and ensure that each has visibility at a senior level. Monitor all actions taken, and once the appropriate measures are in place, ensure they are tested continuously and audited regularly.

“Data breaches can lead to heavy financial losses and serious reputational harm. At its worst, this damage may even threaten the survival of the company, which makes cyber-security a C-level concern”

Ultimately, the aim should be to embed cyber-security into all business processes. This won’t stop your company from becoming a target, but it will allow you to withstand the inevitable attacks with minimal loss.

There are a number of key considerations for improving cyber-security. First, data breaches can lead to heavy financial losses and serious reputational harm. At its worst, this damage may even threaten
the survival of the company, which makes cyber-security a C-level concern. Someone on the board must have direct responsibility for security and all directors should understand and be familiar with the issues.

Entry points

Those responsible for the organisation’s data and infrastructure must understand the potential entry points for criminals and the exit points for sensitive information. This requires a comprehensive audit of data handling and business practices, across the whole organisation. Where vulnerabilities are identified and business requirements mean they can’t be eliminated, they must at least have judiciously designed controls built around them. Of particular concern to any business are:

- File sharing — whether via portable storage or cloud-based services – is a major threat and needs to be carefully controlled. Particular consideration should be given to how to handle visiting contractors and other third-party representatives.
- External third-party sites and services must be properly vetted and access to them regulated by appropriate network controls and traffic management.
- Staff in relatively junior roles often need access to sensitive data in order to do their job. Systems should contain built-in safeguards to restrict access as required and to alert on unusual activity (like attempting to access many records at once).
- Many organisations collect customer information as a matter of routine, without considering the potential consequences of losing it. This data has a lot more value to cyber-criminals than many companies realise and attitudes around it need to change. Personally identifiable information (PII) ought only to be stored if it is necessary to do so. Where sensitive data really does need to be collected and stored, it must be encrypted.

All security policy needs to begin with the understanding that no technology is foolproof and user actions are the most likely cause of a data breach. Unfortunately, users will often respond negatively to procedural changes, no matter how justified they are from a security point of view. This must be allowed for when implementing cyber-defences. Additional considerations include:

- New security measures will be unsuccessful if they impinge on people’s ability to do their jobs. Either the business suffers, or staff will find a way to circumvent the controls, making the organisation vulnerable again.
- Training on its own is insufficient: just telling people to do something does not make it so. Users must be made fully aware of the dangers the training is intended to prevent. This should include crisis modelling, or some other means of providing them with direct experience of the threat.
- It is hard to maintain a state of perpetual readiness. When security measures are effective, the risk appears to recede. Nobody experiences the threats they’ve been warned about and complacency creeps in. For this reason, rules must be strictly enforced to deter any attempts to subvert them and all protective measures should be reviewed regularly and tested continuously to ensure that they remain effective.

About the author
Matt Eddolls is head of risk change at CoreStream (www.corestream.co.uk), where he is responsible for growing the company’s change management practice and managing its digital governance proposition. He has 10 years of management consultancy experience gained with Deloitte and Accenture. In 2006, Eddolls co-founded CoreStream, initially with a focus on helping large financial services clients adapt their risk systems with the raft of new regulatory changes facing their industry.

References