ComputerWeekly.com | TechTarget

E-guide

CW+ Content

Top 10 cyber crime stories of 2018

In this e-guide:

The year of 2018 was marked by several reports on the spiralling cost of cyber crime to businesses as well as to the national and the global economy, as the cyber security industry turned to the bottom line as a motivator for decision makers to prioritise defence against cyber criminal activities.

The focus on the cost of cyber crime also highlighted the profits to be made by cyber criminals, who more than ever before have organised their operations along the same lines as conventional business to take advantage of shared efforts and economies of scale.

Given the financial incentives, it is unsurprising that 2018 saw the continued increase of cyber crime globally, with crimes in this category up 63% in the UK alone.

This led the National Cyber Security Centre (NCSC) to conclude that the cyber crime to business had reached its highest level to date and government to urge businesses to take action to

reduce the likelihood of becoming victims with the volume, and in some case level of sophistication, of cyber attacks increasing as the lines between cyber criminal and nation state attacks continued to blur.

Another hallmark of cyber crime in 2018 was the rapid rise of cryptojacking as a means of making money for cyber criminals, overtaking ransomware as the most popular cyber crime type. At the same time, 2018 saw increased warnings from security researchers about potential attacks against critical infrastructure.

Unsurprisingly, cyber crime investigations also saw an upward trend this year as UK police reskill to tackle this rapidly growing category of crime, which was identified towards the year's end as one of the most significant harms facing society by a top cyber cop, who reiterated calls earlier in the year for business to become more proactive about fighting and reporting cyber crime.

In another retrospective of the year, the Cabinet Office said the UK's National Cyber Security Strategy is "making good progress", but acknowledged that there is still much work to be done, calling on UK businesses to join forces with government and each other in raising cyber defence capability.

Warwick Ashford, security editor

Contents

Economic impact of cyber crime is significant and rising

Warwick Ashford, security editor

Businesses need to take the economic impact of cyber crime more seriously, say researchers, with the cost of cyber crime now up to 0.8% of global gross domestic product (GDP) or $600bn a year, a study has revealed.

This is up from 0.7% of GDP in 2014 and represents a 34% increase from $445bn, which is an average rise of 11.3% a year for the three years to June 2017 – steady and significant growth.

Europe suffers the highest economic impact of cyber crime, which is estimated at 0.84% of the regional GDP, compared with 0.78% in North America, according to the latest report on the economic impact of cyber crime by security firm McAfee and the Center for Strategic and International Studies (CSIS).

The main drivers of this growth include the easy availability of cyber crime tools, the rapid adoption of new technologies by cyber criminals, the expanding number of cyber crime centres, and the growing sophistication of top-tier cyber criminals.

“There is a serious problem with under-reporting of cyber crime, with up to 95% going unreported, so the $600bn figure is extremely conservative and is based purely on the figures we have available,” said Raj Samani, chief scientist and fellow at McAfee. “It is bound to attract criticism, but people need to look beyond the metrics at the real story of how the economic impact is growing, and they will realise that it has value because, all of a sudden, we begin to get a different debate.

“The cost of doing business in the digital age is to protect your IT systems and investments, and the economic impact of cyber crime should be one of the most important things businesses are focusing on because failure to protect their intellectual property [IP], financial information and IT networks does have an economic impact.”

According to Samani, too much attention is paid to which country or cyber crime group is behind attacks to identify who is to blame, whereas the more important focus should be on the economic impact, how that can be reduced and the return on investment in cyber defences.

“The reality is that cyber crime is just an evolution of traditional crime and has a direct impact on economic growth, jobs, innovation and investment,” he said. “Companies need to understand that in today’s world, cyber risk is business risk.”

IP theft alone accounts for at least 25% of the cost of cyber crime and threatens national security when it involves military technology, the report said.

“IP theft and loss of opportunity are two areas of cyber crime impact that are extremely difficult to measure, but we have seen that IP theft and lost opportunities can be fatal for companies, especially for small and medium-sized businesses,” said Samani.

The report identifies cyber crime-as-a-service as a key driver of cyber crime, noting that the industry has become more sophisticated, with flourishing markets offering a broad range of tools and services, such as exploit kits, custom malware and botnet rentals.

“Ever since cyber crime services became commercialised in the mid-2000s, this market has grown and evolved to become bigger and more accessible than it has ever been, with the result that even an 11-year-old could mount and run a ransomware campaign,” said Samani.

Crimeware-as-a-service has not only lowered the barrier to entry, but cyber criminals can now outsource much of their work to skilled contractors, said Steve Grobman, chief technology officer at McAfee.

“Ransomware-as-a-service cloud providers, for example, efficiently scale attacks to target millions of systems, and attacks are automated to require minimal human involvement,” he said.

Add to these factors cryptocurrencies, which ease rapid monetisation while minimising the risk of arrest, said Grobman, and it is clear that recent technological accomplishments have transformed the criminal economy as dramatically as they have every other part of the economy.

Stealing cryptocurrency

Although ransomware is the fastest-growing cyber crime tool, with more than 6,000 online criminal marketplaces and ransomware-as-a-service gaining in popularity, Samani said cyber attackers seeking easy financial gains are increasingly following the money and switching their focus to stealing cryptocurrency.

“Attacks on cryptocurrency exchanges and vaults are fast emerging as a new area of growth for cyber criminal activity, along with associated fraud,” he said.

Greater standardisation of threat data and better coordination of cyber security requirements would improve security, particularly in key sectors such as finance, according to the report, which noted that banks remain the favourite target of cyber criminals.

However, nation states are the most dangerous source of cyber crime, the report said, with Russia, North Korea and Iran being the most active in hacking financial institutions, and China the most active in cyber espionage.

“Our research bore out the fact that Russia is the leader in cyber crime, reflecting the skill of its hacker community and its disdain for western law enforcement,” said James Lewis, senior vice-president at CSIS.

The UK recently attributed to Russia the NotPetya malware attacks that affected companies around the world in June 2017, declaring that the UK and its allies will not tolerate malicious cyber activity.

“North Korea is second in line, as the nation uses cryptocurrency theft to help fund its regime,” said Lewis, “and we are now seeing an expanding number of cyber crime centres, including not only North Korea but also Brazil, India and Vietnam.”

The types of cyber crime that have the biggest economic impact include:

- The loss of IP and business-confidential information.
- Online fraud and financial crimes, often the result of stolen personally identifiable information.
- Financial manipulation directed toward publicly traded companies.
- Opportunity costs, including disruption in production or services and reduced trust in online activities.
- The cost of securing networks, buying cyber insurance and paying for recovery from cyber attacks.
- Reputational damage and liability risk for the affected company and its brand.

The report also includes some recommendations on how to deal with cyber crime, including:

- Uniform implementation of basic security measures and investment in defensive technologies.
- Increased cooperation among international law enforcement agencies.
- Improved collection of data by national authorities.
- Greater standardisation and coordination of cyber security requirements.
- Progress on the Budapest convention on cyber crime.
- International pressure on state sanctuaries for cyber crime.

Next Article

Business cyber crime up 63%, UK stats show

Warwick Ashford, security editor

There were 4.7 million incidents of fraud and computer misuse in the 12 months to September 2017, a 15% decrease from the previous year, according to the latest crime figures for England and Wales.

Fraud fell from 3.6 million in 2016 to 3.2 million incidents in 2017, while computer misuse dropped from 2 million incidents in 2016 to 1.5 million in 2017, according to data gathered from the Crime Survey for England and Wales (CSEW) (households), and the National Fraud Intelligence Bureau (NFIB) (business).

The fall in fraud was driven mainly by decreases in consumer and retail fraud, such as offences related to online shopping or fraudulent computer service calls, the ONS report said, while the fall in computer misuse was mainly due to a 26% fall in reported incidents of computer malware and distributed denial of service (DDoS) attacks.

However, the report also reveals that 56% of fraud incidents were cyber related, 23% of computer misuse incidents (410,000) involved loss of money or goods

relating to computer malware and DDoS attacks, and computer misuse crime referred to the NFIB by Action Fraud increased by 63%.

This rise in business-related computer misuse to 21,745 offences, the report said, is largely accounted for by a 145% rise in computer malware and DDoS attacks the past year to 8,292 offences.

More specifically, this is thought to be due to a rise in levels of malware, mainly ransomware and Trojans, including several high-profile attacks and security breaches on national institutions, including the WannaCry attacks in May 2017.

The latest figures suggest that while consumer-targeted attacks might be falling, as consumer-grade security improves, cyber criminals are now shifting their gaze to the potentially more profitable enterprise sector.

Andy Waterhouse, pre-sales director for Europe at RSA Security, said UK business is facing tougher conditions than ever as cyber attackers chase greater profits.

“In this post-WannaCry world, both consumers and organisations need to do more to assess their data, identify their most valuable assets, and protect these ‘crown jewels’ as best they can through a mix of multi-factor authentication, strong and unique passwords and a greater level of education on cyber skills,” he said.

Fraser Kyne, European CTO at Bromium, said the increase in in computer misuse incidents involving business is no surprise given the spate of ransomware and Trojan attacks in the past year.

“Last year was a year of mega-breaches that made clear how far ahead the bad guys are compared to the security industry. Businesses were shut down for long periods of time, too many ransoms were paid, the bad guys got richer and the security industry looked on, often powerless, as its tools were rendered useless by new and constantly evolving techniques,” he said.

However, Kyne said it was worth noting that this the ONS figures related only to reported crime. Reports can only tell us what has been detected and reported.

“These detected events prove that things are getting in; so we must also assume that things are getting in that are remaining undetected too. This is why we need tools that can protect us from the things that we can’t see or detect,” he said.

“Cyber crime will continue to flourish as long as the security industry remains reliant on detection-based security tools. With cyber criminals becoming more successful every year, we have to admit that the detection model is broken.

“The industry must respond with new ways of defending enterprises and the public at large to ensure that we don’t see the continued rise of cyber crime.”

According to Kyne, virtualisation can provide this protection to enterprises. “By running applications within their own completely isolated virtual machine, you can ensure that any malware directed at businesses is contained to that environment, unable to escape and infect the rest of the system.”

Josh Gunnell, fraud specialist at the Callcredit Information Group, said the latest ONS statistics clearly indicate that fraud remains a threat to every organisation in the country.

“With 3.2 million incidents of fraud in England and Wales and 1.8 million being cyber related, the worrying trend shows no signs of abating,” he said.

“This is especially pertinent considering the damaging impact the ongoing fraud threat has had on trust in organisations, with a majority of consumers we spoke to believing that fraudsters are always one step ahead of businesses.

“To win back consumer confidence, which is key to long-term success, businesses need to do everything they can to keep data and identities safe. Implementing smarter, more dynamic fraud prevention strategies, such as artificial intelligence, alongside traditional fraud prevention methods – and communicating these to their customers – can go a long way towards achieving this. In addition, the importance of using behavioural and location data to provide fraud insights cannot be overstated,” he added.

Cyber threat to UK business greater than ever, report reveals

Warwick Ashford, security editor

Criminals are carrying out more online attacks on UK businesses than ever before, according to the latest joint cyber threat report by the National Cyber Security Centre (NCSC) and the National Crime Agency (NCA) in collaboration with industry partners.

Publication of the *Cyber threat to UK business industry 2017-2018* report coincides with the start of the three-day CyberUK 2018 conference in Manchester that is to be attended by more than 2,200 specialists from across government, industry and law enforcement.

The report details some of the biggest cyber attacks from the past year and notes that risks to UK businesses continue to grow in terms of financial loss, reputation damage and even physical harm as was seen in the global WannaCry attack that affected the NHS.

Emerging threats are also highlighted, such as theft from cloud storage and the hijacking of computers for illicit cryptocurrency generation. This is in addition to the fact that supply-chain compromises of managed service providers and

legitimate software such as MeDoc and CCleaner have provided cyber adversaries with a potential stepping stone into the networks of thousands of companies.

“It is clear that even if an organisation has excellent cyber security, there can be no guarantee that the same standards are applied by contractors and third-party suppliers in the supply chain,” the report said.

According to the report, a basic cyber security posture is no longer enough, but most attacks will be defeated by organisations that prioritise cyber security and work closely with government and law enforcement.

The key to better cyber security is understanding the problem and taking practical steps to reduce risk, according to Ciaran Martin, chief executive of the NCSC, which was created as part of the five year National Cyber Security Strategy (NCSS) announced in 2016 and supported by £1.9bn in investment.

“This report sets out to explain what terms like cryptojacking and ransomware really mean for businesses and citizens, and using case studies it shows what can happen when the right protections aren’t in place,” he said.

The NCSC is the cyber arm of GCHQ, a leading technical authority on cyber security. Since launching in October 2016, it has responded to more than 800 incidents and its Active Cyber Defence programme has blocked more than 54 million malicious emails spoofing government departments.

Growing cyber threat

Martin notes in the foreword to the report that the past year has seen no deceleration in the tempo and volume of cyber incidents, as attackers devise new ways to harm businesses and citizens around the globe.

However, despite these threats to the nation's security, he said he is "confident" in the UK's ability to combat the attacks that organisations face every day. The report underlines that failure to do so could result in the crippling of smaller organisations and significant loss in stock market value for powerful multinational organisations if they lose the personal data and trust of customers.

"The NCSC's aim is to make the UK an unattractive target to cyber criminals and certain nation states by increasing their risk, and reducing their return on investment," wrote Martin. "We have adopted a proactive approach to dealing with the increasingly challenging cyber landscape and in tandem with the NCA are taking a proactive approach to combating cyber crime.

He added: "Together with our law enforcement colleagues from the NCA, the technical experts here at the NCSC have been instrumental in helping citizens and organisations of all sizes protect themselves with the aid of guidance and other bold initiatives like the Active Cyber Defence programme.

“My hope is that by sharing our experiences of exposure to cyber incidents, we raise awareness across the board and, as a result, improve the nation's cyber defences for good.”

The report notes that UK firms are under increasing threat from ransomware, data breaches and supply-chain weaknesses, which can mean serious financial and reputational damage.

It cites real-life case studies from businesses damaged by cyber crime, including ransomware attacks that have affected companies ranging from multinational firms to independent restaurants.

Cyber crime under-reported

While law enforcement and government have battled many cyber threats in the past year successfully, the report highlights that under-reporting of cyber crime by businesses means crucial evidence and intelligence about cyber threats and offenders is lost.

Donald Toon, director of the NCA’s Prosperity Command, which covers economic crime and cyber crime, said organisations that do not take cyber security extremely seriously in the next year are risking serious financial and reputational consequences.

“By increasing collaboration between law enforcement, government and industry, we will make sure the UK is a safe place to do business and a hostile

zone for cyber criminals," he said. "Full and early reporting of cyber crime to Action Fraud will be essential to our efforts."

The NCA hosts the National Cyber Crime Unit (NCCU), which leads the UK's law enforcement response to the cyber threat. NCCU deputy director Oliver Gower said the report not only underlines the fact that the cyber threat is increasing, but also that organisations and individuals have social responsibility to report cyber crime to enable law enforcement officers to carry out investigations.

However, he expects that after the compliance deadline on 25 May 2018, the EU's General Data Protection Regulation (GDPR) will have a significant and positive effect on improving security around personal data and driving up cyber crime reporting, because of the mandatory personal data breach reporting it requires and the heavy fines that can be imposed for failing to do so.

"We are working with the Information Commissioner's Office [ICO] around encouraging organisations that report breaches under the GDPR to also report any associated cyber crimes to Action Fraud," he told Computer Weekly, pointing out the organisations will also be required to report to the ICO if personal data they hold is rendered inaccessible due to a ransomware attack, for example.

As a positive consequence of GDPR breach reporting, Gower said UK law enforcement is preparing for an increase in cyber crime reporting against a background of increasingly aggressive, smart and agile cyber threats.

“We are pleased with the investment we have been able to secure from government to sustain and improve the capabilities of the NCA and UK policing in general to cope with more scenarios like WannaCry,” he said.

In terms of preparing for increased cyber crime reporting, Gower said the NCA has looked at projected cyber crime levels in the context of the different grades of cyber attacks affecting UK business to calculate the resource levels required.

“So that means having more forensics officers, more intelligence officers, more investigators and more sustained relationships with industry,” he said.

Improving legislation

At the same time as increasing capacity, Gower said the NCA is working with government on improving legislation to ensure tougher and more appropriate sentences for convicted cyber criminals to serve as a greater deterrent to would-be cyber criminals.

In the past year, he said, UK law enforcement has demonstrated its increased capacity with 100 arrests of suspected cyber criminals in 2017, a 30% increase in actions aimed at disrupting cyber criminal operations and support services

such as money laundering, and more convictions and work against cyber crime than ever before.

“Policing is being modernised and as a result cyber criminals are not anonymous and we are increasing our proactive capabilities to improve our rates of arrest and conviction, with law enforcement departments dealing with cyber crime including more coders, architects and data scientists working alongside investigators,” said Gower.

According to the NCSC, CyberUK 2018 includes state-of-the-art industry and government displays on the exhibition floor demonstrating cutting-edge technology to help the UK thrive in the digital age. This is as well as a series of lectures, keynotes, panel debates and workshops relating to the NCSC’s four objectives of nurturing cyber skills and understanding, reducing and responding to attacks.

Next Article

Government urges UK businesses to beef up cyber crime defences

Warwick Ashford, security editor

More than four in 10 UK businesses suffered a data breach or cyber attack in the past 12 months, according to the government's latest *Cyber security breaches survey* report.

With just one month to go until new data protection laws come into force, UK businesses are being urged to protect themselves, with statistics showing that more than four in 10 businesses (43%) and two in 10 (19%) charities suffered a cyber breach or attack in the past year.

This figure rises to more than two-thirds for large businesses, 72% of which identified a breach or attack in the past year. For the average large business, the financial cost of all attacks over the past 12 months was £9,260, with some attacks costing significantly more, according to the report based on a survey of more than 1,500 UK businesses and 569 UK registered charities.

The most common breaches or attacks were via fraudulent emails, often attempting to trick staff into revealing passwords or financial information, or

opening dangerous attachments. These were followed by instances of cyber criminals impersonating the organisation online, then malware and viruses.

Minister for digital and the creative industries Margot James said: “We are strengthening the UK’s data protection laws to make them fit for the digital age, but these new figures show many organisations need to act now to make sure the personal data they hold is safe and secure.

“We are investing £1.9bn to protect the nation from cyber threats and I would urge organisations to make the most of the free help and guidance available for organisations from the Information Commissioner’s Office [ICO] and the National Cyber Security Centre [NCSC].”

As part of the government’s Data Protection Bill, James said the ICO would be given more power to defend consumer interests and issue higher fines to organisations, of up to £17m or 4% of global turnover for the most serious data breaches. The bill requires organisations to have appropriate cyber security measures in place to protect personal data.

“The government is also introducing regulations to improve cyber security among the UK’s critical service providers in sectors such as health, energy and transport, and we have established the world-leading National Cyber Security Centre as part of plans to make the UK one of the safest places in the world to live and do business online,” she said.

Ciaran Martin, CEO of the NCSC, said: “Cyber attacks can inflict serious commercial damage and reputational harm, but most campaigns are not highly sophisticated.

“Companies can significantly reduce their chances of falling victim by following simple cyber security steps to remove basic weaknesses. Our advice has been set out in an easy-to-understand manner in the NCSC’s small charities and business guides.”

The new statistics also show, among those experiencing breaches, that large firms identify an average of 12 attacks a year and medium-sized firms an average of six attacks a year.

Smaller firms are still experiencing a significant number of cyber attacks, with more than two in five micro and small businesses (42%) identifying at least one breach or attack in the past 12 months, which could affect profits and reduce consumer confidence, the government report said.

Raft of cyber security advice freely available

However, the survey shows more businesses are now using the government-backed, industry-supported Cyber Essentials scheme, which the government describes as a “source of expert guidance” showing how to protect against cyber threats.

The survey reveals that nearly three-quarters of businesses (74%) and more than half of all charities (53%) rank cyber security as a high priority for their organisation's senior management.

Organisations have an important role to play to protect customer data, the government said. Small businesses and charities are urged to take up tailored advice from the National Cyber Security Centre. Larger businesses and organisations can follow the 10 steps to cyber security for a comprehensive approach to managing cyber risks and preventing attacks and data breaches.

Organisations can also raise their basic defences and significantly reduce the return on investment for attackers by enrolling on the Cyber Essentials initiative and following the regularly updated technical guidance on Cyber Security Information Sharing Partnership and the NCSC website.

Raj Samani, chief scientist and fellow at security firm McAfee said that unfortunately, awareness of government initiatives and communications around cyber security remained low.

"Just 3% recalled using government information, advice or guidance, with most organisations unaware of most initiatives," he said. "Given that 84% of organisations that used government resources found the information useful, it is clear that more needs to be done to promote their use. With such a wealth of information and partnerships with leading security providers, it is imperative that

more is done to promote and educate businesses on what resources they have and how it can help."

Information commissioner Elizabeth Denham said: "Data protection and cyber security go hand in hand: privacy depends on security.

"With the new data protection law, the General Data Protection Regulation (GDPR), taking effect in just a few weeks, it's more important than ever that organisations focus on cyber security. That's why we've been working with the Department for Culture, Media and Sport (DCMS) and the NCSC to offer practical security steps that organisations can consider to keep data safe.

"We understand that there will be attempts to breach systems. We fully accept that cyber attacks are a criminal act. But we also believe organisations need to take steps to protect themselves against the criminals. I'd encourage organisations to use the new regulations as an opportunity to focus on data protection and data security," she said.

Organisations which hold and process personal data are urged to prepare and follow the guidance and sector FAQs freely available from the ICO. Its dedicated advice line for small organisations has received more than 8,000 calls since it opened in November 2017, and the Guide to the GDPR has had over one million views. The ICO also has a GDPR checklist, and 12 steps to take now to prepare for GDPR.

The survey also revealed that larger businesses and charities were more likely to identify cyber attacks, and breaches were more likely to be found in organisations that hold personal data and where employees use their personal devices for work.

Organisations still neglecting basic security

Unsurprisingly, the survey data shows that a huge proportion of all organisations are still failing to get the basics right. A quarter of charities are not updating software or malware protection, a third of businesses do not provide staff with guidance on passwords, and more than one in 10 (11%) of large firms are still not taking any action to identify cyber risks, such as health checks, risk assessments, audits or investing in threat intelligence.

Peter Carlisle, vice-president for Europe at Thales eSecurity, said that although the report reveals that businesses and charities have certain cyber security controls in place, it is “worrying” that only 37% of businesses encrypt personal data, with the figure being just 31% for charities. “Data encryption should be considered a minimum level of security for organisations, as all data will then be rendered useless in any kind of breach or leak.

“According to our *Global data threat report*, over a third of organisations have suffered a data breach in the past year, and with the GDPR coming into force in a month’s time, companies need to ensure that they have taken the required steps to protect all data or risk facing devastating fines,” he said.

Also on the topic of security controls, James Romer, chief security architect for Europe at SecureAuth, said many of the threats organisations were facing could be addressed through complete identity management platforms, combining identity access controls alongside user awareness programmes.

"It appears from the report that businesses and charities have not correctly identified the importance of implementing strategic identity solutions as a priority to improve their cyber defences. It's clear that with identity and credentials accounting for the majority of data breaches, more awareness and focus needs to be put on comprehensive authentication techniques to shore up organisations' defences and prevent cyber attacks in the future," he said.

Organisations need to go further than just two-factor authentication, said Romer, using identity platforms that join silos of data together to create comprehensive identity controls. "Part of those controls should be to implement adaptive authentication that combine techniques such as geographic location analysis, device recognition, IP reputation-based threat services, and phone fraud prevention to address the threats at the identity level efficiently," he said.

Greg Day, vice-president and chief security officer for Europe at Palo Alto Networks, said the report shows that very little has changed from previous years. "While there are some positive improvements since the last report, in particular more regular senior level engagement, generally it is disappointing because virtually all UK businesses rely on some form of digital communication or services, and the frequency of attacks is edging up.

“It’s really important that businesses get basic hygiene right, otherwise you’re just putting hard work, customer data and day-to-day business operations at risk. We need to establish whether the problem is due to lack of knowledge, skills or resource, or a combination of all three.

“Traditional cyber security mindsets have created a heavy human workload, which take up resources. But we’re now seeing new legislation which leverages the concept of state-of-the-art cyber security that allows for much greater automation and efficiencies.

“As such, businesses need to consider if they have a modern, state-of-the-art security operating platform or a legacy of components. For resource-poor businesses, the cyber security industry has started to offer security as a service, so businesses that don’t have the skills internally can leverage others,” he said.

On the topic of cloud security, Day said the report tallies with Palo Alto research that security policies cover cloud computing only 59% of the time. “This rush to the cloud is not taking full account of the security risks. We know from our own research that despite most cyber security professionals (64%) saying security is a top priority for their adoption of the public cloud, less than half of respondents are very confident that existing cyber security in the public cloud is working well, and only 19% of those we spoke to said they had the correct level of involvement in the security of cloud services,” he said.

Visibility is critical to IT security, said Day, but the move to the cloud has brought with it multiple suppliers and new responsibilities for security, which is making visibility harder. “Our research found that only around one in 10 (13%) cyber security professionals said they were able to maintain consistent, enterprise-class cyber security across their cloud(s), networks and endpoints. If we can’t see or understand what good looks like, and can’t consistently apply controls to enable our increasingly digital businesses, then we should expect future reports to only get worse. The capabilities and opportunities are there for improvement – businesses just need to take them.”

Security awareness needs effort

Laurance Dine, managing principal, investigative response at Verizon, said it was particularly noteworthy that around three-quarters of all breaches were linked to staff receiving fraudulent emails, indicating there is still much work to be done on employee education.

“Employee awareness schemes are critical to ensuring staff are equipped with the ability to spot fraudulent emails and learn to be more cynical to keep the organisation safe, so it’s a concern that just one in five businesses have such training in place,” he said.

Piers Wilson, head of product management at Huntsman Security, said that just as we do not let people drive without getting their licence, every untrained employee could pose a threat. “It should be about helping staff see why those

are necessary and the consequences of ignoring them. Right now, too many people just see security as something that blocks them from doing their job rather than keeping the business safe. Until that changes, security is going to remain an afterthought and we'll continue to see reports like this."

Rashmi Knowles, field CTO for Europe at RSA Security, said it was worrying that despite most UK businesses claiming cyber security is a high priority, less than a third of businesses give cyber security responsibility to a board member. "Only 35% employ information security staff, cyber security training programmes are pretty scarce, and less than three in 10 businesses have a security policy in place. It's no surprise we are seeing so many businesses get hacked.

"Organisations need to stop paying lip service and start putting the right people, processes and technologies in place to manage this risk to their business. The worlds of security and risk are converging, and organisations desperately need to recognise that cyber security is a business problem – it's no longer acceptable to feign ignorance, or claim that your business isn't at risk, as one in five UK businesses have claimed this year.

"With GDPR just a month away, organisations are in for a rude awakening, as the costs outlined in this report are likely to skyrocket over the next 12 months. Businesses simply can't afford to wait until a breach occurs to start taking security seriously. Organisations need to take a business-driven approach to security, where they assess their most important assets and scale security accordingly, to ensure a company's most important assets, such as IP and

customer data, are secured through layered security, multifactor authentication, advanced threat detection and complete visibility of IT infrastructure," she said.

Next Article

Nation state cyber attacks affect all, says former GCHQ boss

Warwick Ashford, security editor

High-level nation state cyber threats are a problem for all organisations either directly or indirectly through cyber crime groups acting as state proxies, according to Robert Hannigan, former director general of GCHQ.

“We are seeing a cross over between nation states and criminal groups acting on their behalf, sometimes with the same people working on nation state cyber activities by day and criminal activities by night,” he told Infosecurity Europe 2018 in London.

“However, most cyber attacks, even the most sophisticated nation state attacks, exploit the same things – namely poor patching, network configuration and password management, –so simply by doing the basics properly, 80% to 90% of attacks can still be prevented or mitigated,” he said.

The other piece of good news, said Hannigan, is that most company boards now understand the importance of good cyber security and are planning to invest more in this area, and this has been accelerated by the need to comply with the General Data Protection Regulation (GDPR).

Hannigan said he was also encouraged and delighted by the success of the National Cyber Security Centre's Active Cyber Defence Programme.

"This is being piloted in government with the plan of rolling this out nationally through internet service providers. This programme is demonstrating that it is possible to take effective measures at a national level, and the UK is leading the way internationally in this kind of experimentation," he said.

A commoditised industry

One of the biggest changes in recent years that Hannigan highlighted is the fact that cyber criminals no longer need technical skills to mount attacks.

"The number of cyber crime actors and cyber attacks is increasing mainly due to the availability of cyber crime tools and services on the deep or dark web," he said. "Cyber attacks are now cheaper and easier than ever, and that has helped to escalate the threat."

This commoditised industry is being driven by organised crime groups that are able to pull in whatever skills they need from anywhere in the world, said Hannigan.

"The commodity crimeware market is the ultimate gig economy. It is a powerful business model, and the top groups have an impressive agility in moving from one money making opportunity to the next," he added.

However, Hannigan said cyber criminals typically go after the easiest, softest targets. “For cyber defenders, this means it is really about hardening everything to the point that it is not worth the attacker’s effort rather than achieving perfection,” he said.

Defenders also need to be aware that attackers are now scanning for common vulnerabilities, said Hannigan, which means they will strike wherever they find an opportunity, adding that this is an area where attackers are most likely to start using artificial intelligence (AI) technology.

“Many companies that thought that they were below the radar have woken up to this threat when they became collateral damage, because they had the same vulnerabilities in their networks as attack targets,” he said.

Threat of nation state attacks

Returning to the topic of nation state attackers, Hannigan said the main actors are North Korea, Iran and Russia.

While North Korea is focused on stealing foreign currency in the digital world as it is in the physical world, he said Iran is “good at calibrating cyber attacks for effect”, which is why a cyber response is expected if the nuclear deal with six world powers collapses.

“Russia is at the higher end and we have been locked in a cyber conflict with them for a while,” said Hannigan, adding that Russia has invested a significant of time and money in developing its cyber capabilities in the past 10 years.

“Although we have seen Russian activity since the early 90s, what has changed is the decision to weaponise its cyber activity, from disrupting power supplies in Ukraine to disruption election in the US and elsewhere.

“Attacks on utility and energy companies is a great political weapon, and although these attacks use traditional techniques such as spear phishing and watering hole attacks, they are taking these techniques to a new level by sending phishing emails from within company networks and compromising legitimate websites for watering hole attacks,” he said.

Hannigan also expressed concern about the ability for cyber actors to compromise supply chains to infect software updates and equipment.

“A network router is a worrying place to find any unauthorised party, especially if it is a state actor who is willing to do damaging things and who is getting more sophisticated, more brazen and less worried about getting caught,” he said.

In this context, Hannigan said the “risk of miscalculation and unintended consequences is huge” and although no one has been hurt or killed as the result of cyber attacks, if malicious actors are increasingly tampering things such as medical equipment, it is “only a matter of time”.

The current state of the cyber threat landscape, said Hannigan, means that while old the old threats and risks will never go away, organisations need to look at the emerging threats to ensure they are able to counter these in the future.

“New problems will be amplified by the expansion of the attack surface mainly due to the proliferation of devices making up the internet of things,” said Hannigan.

“There is evidence that the market will not self-correct, so we need to find ways of changing that, which could be a mix of legislation. But in the meantime, organisations should be looking at what is connecting to their networks, evaluate the security risk, and mitigate that,” he said.

Hannigan also cautioned organisations about the need to ensure that they are paying enough attention to security in the cloud.

“Many cloud providers claim that data in the cloud is typically safer than on premise, and generally that is true because cloud service providers typically have greater security resources than their customers, but there are caveats – as outlined in NSCS guidance – and organisations should ensure they look at that.”

Next Article

Cyber criminals 'infect and collect' in cryptojacking surge

Warwick Ashford, security editor

The first quarter of 2018 was dominated by growth in illicit cryptocurrency mining, known as cryptojacking, according to the latest cyber threats report from security firm McAfee.

Researchers saw an average of five new threat samples every second in the first three months of the year and notable campaigns demonstrating a deliberate drive to technically improve upon the most sophisticated established attacks of 2017, the report said.

“There were new revelations this quarter concerning complex nation-state cyber-attack campaigns targeting users and enterprise systems worldwide,” said Raj Samani, chief scientist at McAfee. “Bad actors demonstrated a remarkable level of technical agility and innovation in tools and tactics. Criminals continued to adopt cryptocurrency mining to easily monetise their criminal activity.”

Data analysis shows that cyber criminals extended their operations in cryptojacking and other cryptocurrency mining schemes, where perpetrators

hijack victims' browsers or infect their systems to secretly use them to mine for legitimate cryptocurrencies such as Bitcoin.

The category of coin miner malware grew 629% in the first quarter of 2018, up from around 400,000 total known samples in Q4 2017 to more than 2.9 million the next quarter. This suggests that cyber criminals are continuing to warm to the prospect of simply infecting users' systems and collecting payments without having to rely on third parties to monetise their crimes, the report said.

"Cyber criminals will gravitate to criminal activity that maximises their profit," said Steve Grobman, chief technology officer at McAfee. "In recent quarters we have seen a shift to ransomware from data theft, as ransomware is a more efficient crime. With the rise in value of cryptocurrencies, market forces are driving criminals to cryptojacking and the theft of cryptocurrency. Cyber crime is a business, and market forces will continue to shape where adversaries focus their efforts."

The North Korean Lazarus cyber crime ring launched a highly sophisticated Bitcoin-stealing phishing campaign – HaoBao – which targeted global financial organisations and Bitcoin users. When recipients open malicious email attachments, an implant would scan for Bitcoin activity and establishes an implant for persistent data gathering and crypto mining, the report said.

In January, McAfee Advanced Threat Research unit reported an attack targeting organisations involved in the Pyeongchang Winter Olympics in South

Korea. The attack was executed via a malicious Microsoft Word attachment containing a hidden PowerShell implant script. The script was embedded within an image file and executed from a remote server.

Dubbed Gold Dragon, the resulting fileless implant encrypted stolen data, sent the data to the attackers' command and control servers, performed reconnaissance functions, and monitored anti-malware solutions to evade them.

Also in the first quarter, Operation GhostSecret targeted the healthcare, finance, entertainment, and telecommunications sectors. Operation GhostSecret is believed to be associated with the international cyber crime group known as Hidden Cobra.

The campaign, which employs a series of implants to appropriate data from infected systems, is also characterised by its ability to evade detection and throw forensic investigators off its trail. The latest Bankshot variation of GhostSecret uses an embedded Adobe Flash exploit to enable the execution of implants.

It also incorporates elements of the Destover malware, which was used in the 2014 Sony Pictures attack, and the Proxysvc implant, a previously undocumented implant that has operated undetected since mid-2017.

Publicly disclosed security incidents

McAfee Labs counted 313 publicly disclosed security incidents in Q1 2018, a 41% increase over Q4. Incidents involving multiple sectors (37) and those targeting multiple regions (120) were the leading types of incidents in Q1.

The report shows that disclosed incidents in healthcare rose 47%, with cyber criminals continuing to target the sector with the Samsa ransomware, and there were numerous cases in which hospitals were compelled to pay the criminals.

Incidents of attacks on the education sector rose 40%, with ransomware being a notable culprit in attacks on schools and related institutions, while disclosed incidents in the finance sector increased by 39%, which included continuous attacks on the SWIFT banking system.

These attacks were not always region-specific, as was the case in previous years, but McAfee identified activity in Russia, and related reconnaissance efforts in Turkey and South America.

In Q1 2018, McAfee Labs recorded threats showing notable technical developments improving upon the latest successful technologies and tactics to outmanoeuvre their targets' defences. And while PowerShell attacks slowed from its 2017 surge, cyber criminals saw increases in exploits of other benign technologies. For example, the total count of malware that exploits LNK capabilities surged 59% compared with the previous quarter.

Although the growth in new ransomware slowed by 32% in Q1 2018, the Gandcrab strain infected around 50,000 systems in the first three weeks of the quarter, supplanting Locky ransomware variants as the quarter's ransomware leader. Gandcrab uses new criminal methodologies, such as transacting ransom payments through the Dash cryptocurrency rather than through Bitcoin

According to the report, the total number of malware samples grew 37% in the past four quarters to more than 734 million samples, while the total known malware samples grew 42%.

Next Article

Industrial control systems a specialised cyber target

Warwick Ashford, security editor

As cyber attacks on infrastructure providers increase, adversaries who specifically target industrial control systems (ICS) have emerged, according to researchers at Cybereason.

This was one of the key findings of a study that analysed the data collected in a honeypot that was designed to look like a power transmission sub-station of an electricity supplier.

The rapid response to the honeypot showed that some cyber attackers are very familiar with industrial control systems and the security measures that utility providers implement, and that they know how to move from an IT environment to an OT (operational technology) environment.

Just two days after the honeypot went live, researchers said attackers had discovered it, prepared the asset for sale on the dark web and sold it to another criminal entity interested in ICS environments.

Unlike other attackers who buy and sell access to compromised networks, the researchers said the adversaries who accessed the honeypot showed no

interest in more generic and less targeted activity like running botnets for cryptomining, spamming and launching distributed denial of service (DDoS) attacks.

“In this case, the attackers had one intention, which was getting to the OT network,” said Cybereason CISO, Israel Barak.

“The attackers appear to have been specifically targeting the ICS environment from the moment they got into the environment. They demonstrated non-commodity skills, techniques and a pre-built playbook for pivoting from an IT environment towards an OT environment,” he said.

Accessing the OT environment is the ultimate goal of these specialised attackers, the researchers said, because these systems operate the pumps, monitors, breakers and other hardware found in utility providers that could be used to control or disrupt services.

However, despite the attackers’ sophisticated techniques, they made some amateur moves that indicate their approach needs some refinement, according to Ross Rustici, Cybereason’s senior director of intelligence.

He noted that the attackers disabled the security tools on one of the honeypot’s servers, a move that “made a lot of noise” which in a real enterprise would draw the security team’s attention.

“The approach of going after ICS systems and ignoring everything else, as well as living off the network to conduct activity, is a level of sophistication you don’t normally see in honeypots. But they made some mistakes, raising red flags that don’t allow us to put them in that upper echelon of attackers,” he said.

In addition to the IT and OT environments, the honeypot included an HMI (human machine interface), protected by a firewall, connecting the two to allow people in the IT environment to control the OT systems.

To attract attackers, the honeypot also included three Internet-facing servers with remote access services and weak passwords, but nothing else was done to promote the servers to attackers.

However, the researchers said the servers’ DNS names were registered and the environment’s internal identifiers were names that resembled the name of a major, well-known electricity provider that serves both residential and business customers in the US and the UK.

Two days after the honeypot was launched, Cybereason researchers determined that a black market seller had discovered it based on a toolset that had been installed in the environment.

The researchers said the tool, xDedic RDP Patch, is commonly found in assets that are being sold in the xDedic black market. It allows a victim and an attacker to use the same credentials to log-in to a machine simultaneously using RDP

(remote desktop protocol), which would otherwise be impossible because of built in security restrictions.

The seller also installed backdoors in the honeypot servers by creating additional users, another indicator that the asset was being prepared for sale on xDedic, the researchers said.

The backdoors were designed to allow the asset's new owner to access the honeypot even if the administrator passwords were changed.

The honeypot was silent for a week until the asset's new owners connected to it by using one of the backdoors. Based on the actions they took, researchers said the new owners were fully prepared to navigate the ICS environment of an electricity provider.

The first action was to disable the environment's security features, including the Cybereason platform. Cybereason was intentionally installed in a way that made removing it simple. This was a test to gauge the attackers' skills.

After disabling the security software, they used Active Directory to conduct network discovery. They looked at all accounts on active directory and looked for technical data files. These files, which had been planted on the machine, included information like the operational status of devices. These files were exfiltrated from the honeypot.

The attackers also discovered ICS assets like the HMI and controller components for the OT environment. The adversaries were interested only interested in ICS assets and did not access any other systems.

The attackers focused on attempting remote execution on ICS endpoints, and while the firewall prevented them from taking that step, the attackers knew how to circumvent these security measures by using multipoint network reconnaissance.

This approach assumes that different assets in an environment have different firewall policies and the attackers move laterally to multiple assets and run parallel network scans to locate an asset with more relaxed policies around interacting with the HMI and OT computers.

The attackers moved from the honeypot's remote server, to the SharePoint server, to the domain controller, to the SQL server to run network scans to determine if one of these assets would allow them to access the ICS environment. Instead of scanning the full network, attackers focused on scanning for assets that would give them access to the HMI and OT computers, the researchers said.

Cybereason was installed a second time with some hardening, but still below the level that is recommended in a deployed environment. The goal was to further assess the attackers' capabilities. The result was that the hardened version was also disabled.

The platform was installed a third time based on recommended guidelines. To date, the attackers have not been able to deactivate it, according to Cybereason.

“In two days, the attackers got into the environment, conducted reconnaissance aimed at finding an entry point from the IT environment to the OT environment, which is really what they wanted,” said Barak.

Unified security operations centre

He suggests that organisations and companies with ICS environments operate a unified security operations centre (SOC) that provides visibility into both the IT and OT environments because the honeypot demonstrated that attackers are looking to use IT environments as gateways into OT environments.

“Companies may have a network operations centre (NOC) monitoring the OT environment, but a combined SOC lets you see all operations as they move through the network. Having this visibility is important because attackers could start in the IT environment and move to the OT environment,” said Barak.

“Threat hunting is also beneficial because this looks for activity that indicates attackers are already in a company’s environment. Instead of waiting to react to an alert issued by a security tool, threat hunting allows defenders to take a proactive approach to security by detecting adversaries before they cause severe damage to a network,” he said.

The activity observed in the honeypot also suggests an increased risk for operators, according to the researchers because the possibility that this is a trophy taker rather than an advanced persistent threat (APT) actor with training on these types of environments dramatically increases the risk of a mistake having real-world consequences.

They added that many of these systems are old and fragile and even trained hacking units make mistakes that cause failures in these controls.

Hackers seeking to make a name for themselves or simply prove that they can get into a system, they said, are far more likely to cause failures out of ignorance rather than malice, makes incident response and attribution harder more difficult and making it more likely to result in an unintended real-world impact.

Next Article

Cyber crime most significant harm in UK, says top cyber cop

Warwick Ashford, security editor

Cyber crime is the biggest evolving crime type in the UK and beyond in terms of volume and complexity, according to detective chief superintendent Pete O'Doherty, lead of cyber and head of economic crime at the City of London Police.

"But it is difficult to police, because unlike other crimes where there is an offender, victim and location, cyber crime tends to be multi-national. If you look at the globalisation of goods, people and services, and an epic evolution in technology, it is without doubt the most significant harm in the UK," he told the information security track of the International Security Expo 2018 in London.

"I have been a detective my whole career and the training I have been given has not equipped me with the skills and techniques that I need to investigate cyber crimes involving multiple actors in multiple countries," said O' Doherty.

Capability to investigate cyber crime is one of the top challenges, he said, particularly when it comes to cyber dependent crime involving botnets,

distributed denial of service (DDoS) and malware, as opposed to the more traditional types of crime that are cyber enabled.

“The next problem is capacity. In the UK we are pleased to say we police by consent, but cyber, terrorism and economic crimes are not top of the list of what citizens [are worried about]. They are worried about things like anti-social behaviour, so there is a big gap between what the public wants from policing and our national threat strategic risk assessment.

“The challenge for us is finding a way to bridge the gap between the threat intelligence and the public voice if our main aim is to achieve public value.”

The third major challenge, said O’Doherty, is that while law enforcement and locking people up is important, it is not going to solve the problem of cyber crime.

“There needs to be a massive focus on intervention, disruption, security by design and intelligence sharing if we are ever going to make a difference, and we need to start looking for digital skills in our recruitment and selection processes,” he said.

Another necessary change, said O’Doherty, is to increase the use intelligence to find links between cyber criminals and more traditional crimes “to leverage the politics” to get local policing to treat it as a priority. “Al Capone was not put in prison for homicide, but for fraud,” he said.

Adapting to challenges

The switch from using credit cards to cryptocurrencies on the dark web is another challenge for police who are now no longer able to use covert credit cards to buy goods to catch criminals offering illegal goods and services.

In the face of these challenges and the increased use of personal data stealing and illicit cryptocurrency mining malware spread through social engineering emails, O'Doherty said the police are adapting their approach to combating cyber crime.

The first area policing has achieved success is in shutting down websites providing unauthorised access to copyrighted content by cutting off their advertising revenue, which was around $50,000 a month.

The City of London Police stepped in by contacting the website operators, inviting them to contact the police for help to legitimise the business. "If they fail to contact us, we put them on a blacklist sent to UK advertisers who remove their brands from the offending websites, cutting off advertising revenues.

"We then share the intelligence with Mastercard and Visa, who take down the payment enabler so that any money generated can't be generated overseas, and we share the information Europol, Interpol, the FBI and others so that each country can work within its own legal framework to take down offending sites. In this way, we have saved millions of dollars for the [creative arts] industry, we

have dismantled 70,000 websites and over 100 organised crime gangs operating in this space no longer exist."

Cyber Griffin is another initiative by the City of London Police to provide a free service aimed at helping people protect themselves from cyber crime. "Every month, we use the intelligence we receive to brief industry to help organisations to build robust cyber security practices to prevent the external and internal threats from damaging the business.

"We also do incident response exercises in which we map out an organisation's infrastructure, identify the threat vectors and help design internal regimes to prevent the threats," said O'Doherty.

In response to the capability challenges, police forces are building capabilities and volunteers. "There is now the opportunity to become a volunteer police officer called a special constable to work in investigations to use their expertise in risk mitigation and cyber security to help police do a better job."

The use of "direct-entry detectives" is another effective strategy being used by police in combating cyber crime. "Many people want to be a detective, but don't want to walk the beat. So were are currently designing a way for experts to join the police as a detective by 'direct entry' to investigate fraud and cyber crime as a specialism," said O'Doherty.

“We are also in the process of designing a cyber academy to offer courses around, such as cryptocurrency and cyber investigations for policing and law enforcement,” he said.

In an attempt to get public support for investment in cyber crime fighting, O’Doherty said police forces are giving police chiefs and commissioners a profile that “articulates the impact of cyber crime on local people and draws the links between cyber and organised crime to give them the appetite to invest”.

As a result, he said there has been a “massive improvement” in the level of investment being made by policing and the cases that officers are now able to investigate.

Internationally, O’Doherty there is a UK policing representative in the office of the district attorney of New York in the US who shares intelligence about organised crime gangs that operate across the Atlantic to help coordinate investigations.

UK also has a team of specialists dedicated to working with convicted cyber criminals to understand how their crimes were committed with the incentive of getting their prison terms reduced. One success story, said O’Doherty, is about a 22 year old in the US who designed a chipset that enabled him breach voicemail services around the world to access linked computers and servers to access sensitive databases.

“Under this initiative, he helped police design prevention advice that we disseminated to industry and design a mechanism to ensure that this type of attack can never happen again.”

Another key tool in the police arsenal for fighting cyber crime is disruption activity. “Action Fraud, receives about 24,000 reports a month, which policing does not have the capacity to investigate. But we have a capability that identifies bank accounts, email addresses, VoIP platforms and websites linked to fraud and we have a team that disrupts those entities to prevent further offences, and we estimate that through that work we save around £400m from being lost through fraud,” said O’Doherty.

In closing, he said that “partnership” is a key element of everything policing is doing to address the challenges associated with fighting cyber crime. “Partnership with industry, government and education systems. We cannot do it alone.

“We want every victim of crime, which includes businesses to report those crimes, because if we know what the true scale of the problem is, we can start to develop and intelligence-led, coordinated response to cyber crime, which is significantly under-reported, and that is a big problem,” he said.

Next Article

Cyber crime: why business should report it as soon as possible

Warwick Ashford, security editor

Official statistics show that cyber crime is on the rise in the UK, but the size of the problem in the business world is really unknown because not all victim organisations are reporting incidents.

This is for a variety of reasons, including a lack of faith in law enforcement's ability to help, failure to see how reporting a cyber crime has any benefit, belief that the organisation or incident is too small for police to care, reluctance to admit their cyber defences have failed and concerns that reporting a cyber crime will trigger an investigation that will shut down or hamper business operations.

Mike Hulett, head of operations for the National Cyber Crime Unit (NCCU), which leads UK law enforcement's response to cyber crime at the National Crime Agency (NCA) says all these reasons are based on misconceptions about the value of reporting a cyber crime and what businesses can expect.

At the most basic level, there are no incentives to report cyber crime, while in most other kinds of crime, at the very least, there is the incentive of reporting it

to the police so that they can get a case number for insurance purposes, although that is changing," he says, as more organisations take out cyber insurance with companies who typically encourage clients to report whenever they are victims of cyber crime.

Size doesn't matter

No business is immune from cyber crime from the smallest to the largest of organisations, and the police want to hear from victims, no matter the size of their organisation.

"We want all victims of cyber crime to report. Who you are and what has happened is going to affect the scale and nature of the response, but there is no cut-off in terms of size of organisation affected. We want everybody to report, regardless of how large or small the organisation," says Hulett.

As soon as possible

Data breach investigations reveal that some organisations can takeweeks or months to discover a cyber attack, but some cyber criminal activities are identifiable immediately such as distributed denial of service (DDoS) attacks, ransomware and other types of extortion.

The message here is not to delay in reporting cyber criminal activity. "Report as soon as possible, particularly if it is a crime in action. We have much more

chance of being able to help and of being able to catch the criminals responsible if the crime is reported to us while it is taking place," says Hulett.

Yes, but how?

The NCA recognises that it can appear to be a "cluttered landscape" for the businesses' point of view in terms of how to go about reporting a cyber crime, particularly as many organisations will have to report personal data breaches to their data protection authority for the first time under the EU's General Data Protection Regulation (GDPR) and new GDPR-aligned data protection laws in the UK.

But cyber crime reporting is not as difficult as may seem, says Hulett, adding that a lot has been done in recent months to ensure better coordination and communication in the background once a report has been made to ensure the most appropriate law enforcement response in a reasonable timeframe.

"While there are different law enforcement agencies involved behind the front door, it doesn't matter which front door you go through, whether that is the UK's national fraud and cyber crime reporting centre Action Fraud, the National Cyber Security Centre or the local police force. Action Fraud is still the main point for reporting cyber crime, but it is now a 24/7 service either through a call centre or an online reporting tool.

“Previously people have been put off by the fact that it was available only at certain times of the day, but now it is available whenever people have the opportunity to report cyber crime or if a business wants to report a crime in action that is happening very late at night or early in the morning.”

For crimes in action that are reported outside of normal office hours, Hulett says there are methodologies to ensure that cases are referred to the most appropriate agencies. “For crimes in action, we have arrangements in place to refer them directly to the NCA if necessary.” He also advises that in such cases, organisations use the call centre rather than the online reporting tool.

If organisations are being targeted by cyber attacks they believe could be of national significance, they can report such incidents directly to the National Cyber Security Centre (NCSC), but no matter where they choose to report an incident, Hulett says they can rest assured it will be referred appropriately to ensure crimes get the right response at the right time.

“The challenge for businesses is that it is not always obvious whether they are being targeted by criminal or nation state activity, or whether they are merely experiencing some kind of IT issue. No matter where they go to report, there is enough awareness and connectivity behind the scenes to make sure it ends up in the right place,” he says.

An NCSC spokesperson told Computer Weekly that businesses should always report any cyber attacks to the NCSC immediately. "All reports will be dealt

confidentially and the more information a company shares in a timely manner, the better able we are to support them and prevent others falling victim.

"In the event of significant cyber security incidents, we may also be able to provide direct technical support and cross-government co-ordination of response activities.

"Cyber security should be as second nature for businesses as cashing up or locking the doors at night. The NCSC has also published guidance for organisations on improving their cyber security, such as our Small Business Guide."

OK, but why?

The most basic reason for reporting a cyber crime, says Hulett, is that targeted organisations are victims of crime and as such they are entitle to a law enforcement response. "This alone is a good reason to take what help and advice is freely on offer from law enforcement," he says.

The NCA appreciates that many organisations are nervous that by reporting the incident they will receive more publicity than it otherwise would.

"While it is up to the company involved to manage the media where there is a public security breach, they do not have to worry that law enforcement will exacerbate the situation by publicising something that is not already in the public domain," says Hulett.

“Our goal is also to ensure there are consequences for criminals because cyber crime is still seen as a low risk, high reward environment and we need to change that perception by arresting and prosecuting people, and the more cyber crimes that are reported, the greater our chances of catching the relatively few people out there who are enabling cyber criminal activities.”

A key reason for reporting cyber crime, however, is that it enables law enforcement agencies to gather and exchange better intelligence about cyber criminal activity.

“Even if a company decides they do not want to support a prosecution, there is still value in engaging with us so we can see what has happened to the company and how it has been done to build up an aggregated intelligence picture across a number of incidents,” says Hulett.

“The same approach is used with traditional crime. Most burglars don’t get caught based on evidence at a single crime scene. Typically they get caught because police are able to build up a profile from evidence gathered across several crime scenes.”

What will happen?

Organisations affected by cyber crime are often nervous about what will happen after they report an incident to law enforcement, but Hulett says perception is often different from reality.

The first thing to understand, he says, is that not everyone who reports a cyber crime is going to get an instant response.

Just like responses to other crime types, Hulett says law enforcement has to prioritise and when it comes to cyber crimes, crimes in action or crimes that meet a certain threshold in terms of attack type, size and impact typically get top priority and will automatically referred to the NCA, while historical and low-level incidents will be referred to the relevant police force for investigation.

“If for example, a company were to call Action Fraud to report an active ransomware attack in which their systems have been encrypted so that they can’t do anything, Action Fraud would pass it straight on to the NCA’s central TICAT [triage, incident coordination and tasking] team to decide on the most appropriate response,” says Hulett.

The response can be from the NCA itself, one of the regional organised crime units (ROCUs) or the most appropriate police force.

“In a live ransomware scenario, the affected company would get a call from our TICAT team to get as much information as possible about the incident, including details of what systems have been affected and if there has been any contact from those behind the ransomware.”

Although the NCA would prefer organisations to report incidents as a crime to improve the official statistics around such incidents, Hulett says law

enforcement will still provide advice to companies on how to deal with incidents even if they do not want to file an official crime report.

However, he says that if a company does not want to report an incident as a crime orsupport a prosecution, a forensic team will not sent out.

When companies choose to cooperate with law enforcement, Hulett says whoever has been tasked with the incident will engage with the company to find out who the key employees are and where the firm's hardware is located so that the affected systems can be imaged to capture whatever evidence is available in the least disruptive way possible.

"We fully recognise that they are victims or crime and that companies' priority is to get their business up and running as soon as possible so we try to deal with that as sensitively as we can, but at the same time businesses need to understand the importance of imaging servers as soon as possible before the evidence is gone."

Businesses also need to understand that cyber crime investigators will only image their systems to capture evidence, but will not do things like rebuild affected systems or install new servers.

"If those behind the ransomware have contacted the targeted organisation, it opens up the opportunity for law enforcement to engage with them covertly to

try to work out who they are with a view to identifying and arresting them to face prosecution," explains Hulett.

Another concern is that by reporting a cyber crime to law enforcement, organisations lose control over when and how the incident is made public or brought to the attention of regulators, which can also make them hesitant to answer questions from law enforcement about how their systems work for fear of exposing a lack of security controls.

"We will not go public about an incident or share any information with regulators that is not already publicly known about, but we will advise them to report to the appropriate regulators as soon as possible and we will advise them when it is appropriate to warn customers of a potential breach because they may be subject to direct or secondary fraud, but ultimately it is the company's decision," says Hulett.

Ticking time bomb

Although there may be circumstances when investigators will want to delay going public so that they can glean as much information as they can before alerting the criminals, he says that wherever customers are affected, it is a "bit of a ticking time bomb" for the company involved. "Most companies are tuned in to the fact that they have to go public because of the huge potential reputational damage if they are seen to be trying to cover something up.

“If a company delays going public, the moment affected customers start tweeting about it, the company loses control, so there is a very narrow window in which boards have the choice about whether to say something or not.”

Beware of social engineering

In terms of general advice based on the types of investigations the NCA is doing, Hulett says organisations should not underestimate the power of cyber criminals to use social engineering techniques to get the information they need to breach cyber defences.

“Good cyber defences are easily undermined by the compromise of the logon credentials of IT administrators and other employees either through bad password practices such as using a single username and password for several accounts or through social engineering attacks.”

Once cyber criminals are able to get legitimate credentials, Hulett says they can use them compromise business email accounts to commit crimes and to thoroughly explore company networks without detection to gather information about the company, its employees and its data assets before carrying out an attack.

Positive trends

Despite increases in cyber crime, he says the NCA is also seeing a growing number of companies who are good examples. “Those companies that get it

more right than wrong tend to view cyber security as a continuum rather than something that is reviewed only on an annual basis.

“More organisations are also waking up to the fact that physical security and personnel security are linked to cyber security and that there is no point in doing all these things separately,” says Hulett. There is also a growing number of companies that have cyber insurance to help cover the costs of recovering from a cyber attack and getting systems back up and running again.

“Cyber insurance is growing in popularity, and if it is something that encourages general good cyber security practice and increased cyber crime reporting to law enforcement, then we would support that, but companies need to ensure that cyber insurance does not result in a false sense of security and that they are doing everything that they can to prevent a cyber attack and to recover if one occurs.”

Another positive trend, says Hulett, is the growing awareness of the importance of ensuring cyber security throughout the supply chain. “Businesses are increasingly realising that it is just not their own cyber security that you need to take into account, but also the cyber security of their partners as demonstrated by the NotPetya attacks in 2017 when companies three or four stages removed from the original company targeted by the malware were heavily impacted.”

The growing number of high-profile cyber attacks in the news, says Hulett, means people are more aware of what can happen which is having the positive

effect on companies' understanding of the importance of investing in appropriate cyber security.

"Companies' behaviour is improving, and the GDPR [General Data Protection Regulation] is likely to help even further with that because companies that previously have not given much thought to data protection are now starting to pay attention."

As a parting warning, Hulett says companies should ensure that their backup systems are not vulnerable to the kind of attacks that make them necessary, citing the example of one UK company that was downed by a malware attack but was unable to restore its systems because the malware attacked Active Directory so the company was unable to access its data backups.

Next Article

UK cyber security strategy making ‘good progress’

Warwick Ashford, security editor

One of biggest early successes of the National Cyber Security Strategy launched in 2016 is the establishment of the National Cyber Security Centre (NCSC), according to Mark Sayers, deputy director, National Cyber Security Strategy, at the Cabinet Office.

“That was about bringing together our very best intelligence and technical expertise into a single world-leading authority, which has undertaken some pretty pioneering work in its first two years,” Sayers told the information security track of the International Security Expo 2018 in London.

Since the launch of the strategy, said Sayers, the government has continued to invest in, and build, the UK’s cyber capabilities across UK law enforcement to pursue those who carry out cyber attacks, wherever they are.

“We have developed some ground-breaking early-intervention programmes in an attempt to divert those we have identified as at risk of going down the wrong path [of cyber crime], we are inspiring more people to become cyber security experts and entrepreneurs, we have programmes in schools and universities, and we are even working with industry and the voluntary sector on retraining,” he said.

The past year has seen the introduction of the Cyber Discovery Programme for 14 to 18-year-olds, which has already engaged more than 23,000 students, said Sayers.

Another important element of the strategy is building on the UK’s cyber security research base, he said. “We are working to re-establish a proper pipeline of cyber security companies through a range of initiatives to incubate and accelerate these companies, including the new cyber accelerator in London.”

Under the strategy, Sayers said the UK has continued to build the strength of its collaboration around cyber security with its allies.

“We are looking to confront, expose and disrupt hostile activity, and the public attribution we have been doing in the past few months is our way of putting pressure on those who seem to feel that they can act with impunity, as well as promoting our shared vision for an open, peaceful and secure cyber space,” he said.

At the halfway point in delivering the strategy, the UK is “in a good place” in terms of putting in the building blocks necessary to transform the country’s cyber security and resilience, said Sayers.

“But as the threat from criminals and nation states continues to evolve, we must keep innovating and stepping up our game to rise to the challenge,” he said. “The key to achieving this lies in the strength of the partnerships that we create and our ability to demystify cyber security.”

However, translating a broad increased awareness into people taking action remains challenging, he said. “Often it is seen as too difficult, too technical or as someone else’s problem.”

As a result, the government is increasing its focus on helping company boards better understand the risks that they face and the action they can take, and provide leadership in their organisation to ingrain security in the company culture and mindset, said Sayers.

“We are using the Cyber Essentials Scheme to influence organisations that provide products and services to government because we are specifying standards to improve their cyber security, but we are also specifying that they should enforce those standards right through their supply chains,” he said.

“So they are taking a much more active role in protecting the often much smaller businesses in their supply chain by helping them to improve their overall cyber security resilience.”

Sayers noted that there are now more than 550 private sector partners taking part in the government’s national Cyber Aware campaign, which is aimed at encouraging individuals and businesses to take basic steps that will prevent the majority of high-volume, unsophisticated cyber crime.

Looking to the future, Sayers said the focus of the government’s efforts in the next six months will be to address the cyber security skills gap, the government’s cyber security science and technology strategy, and the ambition to make all products and services secure by design.

In terms of reducing the skills shortage, he said the government continues to forge relationships with industry and academia to develop cyber security as a profession and create clear career pathways as well as a more diverse and inclusive workforce.

As part of these efforts, the government plans to publish a comprehensive cyber security skills strategy to set out what needs to be done by 2021 and beyond.

“But this will require the help of the security industry to validate that strategy and help ensure that we have the right approach, and then to realise that vision and make it happen,” said Sayers.

Maximise opportunities and minimise risks

He said the planned cyber security science and technology strategy demonstrates that the national strategy is not only about addressing the need to make the internet safer, but also about ensuring that the UK can maximise the opportunities and minimise the risks of new and emerging technology.

As the internet of things (IoT) expands, the challenge is to ensure that manufacturers can help consumers by building protections in from the design stage, said Sayers.

“We have developed what we think is a world-leading code of practice for consumer internet-connected devices in consultation with international partners and private sector organisations, because our commitment here is to help manufacturers understand how this code of practice will set in the broader standards landscape and make it as straightforward as possible for them to introduce the changes necessary to improve the security of their products,” he said.

The aim of government, said Sayers, is to demonstrate not only that it understands the challenge and the scale of that challenge, but that it is trying to cultivate the right environment for all stakeholders to be collaborative and agile as possible in their response.

“We do not have all the answers and we cannot do this alone, and whatever lies ahead, I want to make sure we are focused on reaching out across organisational, political and geographic boundaries, because to succeed, we need to be more than the sum of our individual parts,” he said.

“We need to harness the fact that we are safer and stronger together.”

Getting more CW+ exclusive content

As a CW+ member, you have access to TechTarget’s entire portfolio of 140+ websites. CW+ access directs you to previously unavailable “platinum members-only resources” that are guaranteed to save you the time and effort of having to track such premium content down on your own, ultimately helping you to solve your toughest IT challenges more effectively—and faster—than ever before.

Take full advantage of your membership by visiting www.computerweekly.com/eproducts

Images; stock.adobe.com