COLLABORATING TO SUCCEED

Victor Acin *reveals why it's time to socialise cyber security*

It's no secret that IT security leaders are under tremendous pressure today. A barrage of commodity threats and increasingly sophisticated targeted attacks imperil the bottom line, corporate reputation and ambitious digital transformation projects. Things have got to the point that, rather than ask what keeps the average CISO awake at night, it would be quicker to determine what doesn't. Charting a course through this minefield is no easy feat, which is why we all need to get better at collaborating. That means security practitioners, of course, but it should also include law enforcement officers, academics, the vendor community and others. Socialising cyber security in this way will help us finally turn the tables on the black hats. It might take time for many stakeholders to change their ways, but with so much at stake, this time is running out.

Digital transformation sits at the heart of most organisations' growth plans today. Cloud and mobile app-based services, IoT systems, AI, big data, DevOp, and more have come together to drive process efficiencies, greater IT and business agility and innovative new products and services. It's no surprise the market is set to be worth a staggering $665billion by 2023.

THE AVERAGE US OR UK COMPANY SHARES SENSITIVE DATA WITH 583 THIRD PARTIES

In practice, digitisation means more information than ever is being stored, processed and generated online – and by increasingly disparate systems. This translates to a broad attack surface for hackers to target: everything from cloud databases to network-attached storage, online file sharing services to traditional email, CRM and ERP apps. On the one hand, employees increasingly expect to use such productivity-enhancing tools at work: 60 percent of under-35s value the ability to work remotely over generous holiday allowances, for example. But they also create extra cyber risk, especially if staff haven't been trained how to use them securely. Almost two-thirds of breaches are said to be the result of human error.

Sometimes digital innovations allow staff to bypass IT controls put in place specifically to protect the organisation. It's increasingly easy for employees to buy smart devices for the office which are connected to the corporate Wi-Fi network, or to open new cloud accounts and migrate sensitive data over. Shadow IT is a real and pressing challenge for CISOs.

Cyber-related risk doesn't stop at the perimeter, however – increasingly it comes from a complex digital and physical supply chain. These often complex networks of suppliers are absolutely vital to the success of most modern businesses, yet if risk isn't properly managed they can be a significant weak link in the corporate security chain.

It's claimed that the average US or UK company shares sensitive data with a staggering 583 third parties. Nearly 60 percent of firms have suffered a breach as a result of this risk exposure and more than three-quarters believe that such incidents are increasing. Third parties may supply code and/or share digital resources. Their employees may have long-term access to the corporate network. A massive breach at US retailer Target, as well as the NotPetya ransomware worm, were caused by supply chain attacks of one sort or another.

Attackers increasingly appear to have the upper hand over white hats, thanks to a vast cyber crime economy said to be worth as much as $1.5 trillion. It provides an endless source of hacking tools, stolen data and other resources as well as a ready-made market on which to sell the spoils of cyber attacks. Passwords are especially key: stolen or weak credentials account for 80 percent of hacking-related breaches, according to one industry report. According to Blueliv data, there was a 50 percent increase in the volume of log-ins stolen by botnets in 2018. Many of these are used in credential stuffing and other automated attacks, which capitalise on the fact that users tend to reuse their passwords across multiple sites. If they happen to share credentials across consumer and corporate accounts, then the organisation could be at risk.

Such tools have become democratised among the criminal community, thanks to the underground economy. It's making it easier across the board for non-technical types to try their hand at hacking: via ransomware attacks, crypto-mining, banking trojans, click fraud and much more. Hacking services for-hire offer everything a budding cyber criminal could need in just a few clicks. One vendor has even spotted attackers using sophisticated tools linked to the notorious Shadow Brokers data dump to spread crypto-mining malware and ransomware. This includes an Eternal Blue-based backdoor and password dumping tool Mimikatz, along with other tools associated with the suspected NSA Equation Group.

Stolen or weak credentials account for as much as 80 percent of all hacking related breaches

That same vendor noted: an 819 percent surge in fileless malware attacks designed to stay under the radar of traditional security tools; 269 million instances of phishing URL detections; a 28 percent rise in BEC attacks; and a 237 percent increase in crypto jacking. In total, it blocked over 48.3-billion unique threats in 2018. But even this was a decline from previous years. Why? Because hackers are increasingly targeting attacks using sophisticated techniques picked up from the Dark Web, as above. With the tools of the few now in the hands of the many, CISOs are under tremendous pressure.

The result is increased risk of devastating data breaches and service outages. A staggering 4.5-billion records were compromised globally in the first half of 2018 alone. The average data breach costs an estimated $3.9-million, but can go much higher in serious cases. A major incident at Equifax has apparently cost the company a massive $1.4-billion so far in clean-up and investigation costs, legal bills, and more.

While Blueliv saw a decline in ransomware campaigns, attackers are still making use of this tactic. An attack on aluminium giant Norsk Hydro earlier this year cost the firm at least £45-million. The GDPR regulates both breaches and ransomware-related outages if personal data is involved. Over 89,000 breaches have been logged in Europe in its first year, and there are signs that UK regulator the ICO is gearing up for some seriously large fines.

Much of the cyber risk already outlined is driven by the need for employees, consumers and organisations to collaborate. However, it's also true that the best way to combat cyber risk is through enhanced collaboration. Yes, best practices will always be important. These include training staff up efficiently, patching promptly, running regular pen tests, restricting user privileges, improving password management, network monitoring, implementing AV and more. They are outlined in documents like the National Cyber Security Centre (NCSC)'s handy *10 Steps To Cybersecurity* guide.

However, for effective, deep defence we all need to improve collaboration. It might come in many forms: for example, finding a threat intelligence vendor prepared to sit down with each individual client to create a bespoke model. Modular, API-based data feeds and ongoing customised intelligence assessments can provide the kind of personalised, collaborative approach that gets results.

Picture credit: Getty

It also means sharing intelligence at an industry level, so that CISOs have access to more accurate threat data. The Blueliv Threat Exchange Network is a global community of thousands of cyber security experts, IT professionals and academics. Each month members publish the latest news, threat data, IOCs and more in order to improve resilience and accelerate incident response. In the UK, the Cyber Security Information Sharing Partnership (CiSP) was created back in 2013 and now sits within the NCSC.

MORE INFORMATION THAN EVER IS BEING STORED, PROCESSED AND GENERATED ONLINE

Hundreds of organisations "exchange cyber threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK business". In the US, meanwhile, the Department for Homeland Security (DHS) works with a number of sector-specific Information Sharing and Analysis Centers (ISACs), including ISACs for aviation, emergency services, health, nuclear, real estate, financial services and oil and gas.

However, law enforcers and intelligence agencies could do more to encourage participation in such schemes. Historically there have been concerns around sharing sensitive threat information in case government spies use it for their own ends, or in case it is leaked, causing reputational damage to the firm. Governments and police need to provide stronger assurances that this will not happen, because without improved participation in such schemes, the societal and economic impact of cyber crime could take an increasingly large toll. Given police cutbacks in many countries, there's a greater need than ever for investigators to pool their resources with private sector firms to help bring cyber criminals to justice.

Information sharing could also happen on a more informal level. That's the value of traditional industry conferences like Infosecurity Europe and RSA Conference. They have been a great place for security practitioners to meet their peers and share war stories and best practices over the years as well as hear from some of the leading lights in the industry on innovations in security technology and the continued evolution of the threat landscape. The concern is that as day-to-day pressures continue to rise, CISOs will no longer be able to get out of the office to attend such events.

In fact, as the industry skills crisis deepens, there's a greater need for collaboration than ever before. Recent research has revealed that European CISOs believe the black hats are winning the cyber skills race. More worrying still, 64 percent of security leaders say they have considered quitting their role, and 63 percent have thought about leaving the industry completely, because of the pressure they're under. We need to regroup and fight back. The bad guys are adept at information sharing to further their nefarious ends. We need to respond in kind, at every level ●

Victor Acin has been working for Blueliv for five years, three of which he has been part of the LABS team where he now acts as Team Lead, performing tasks related to the generation of Threat Intelligence and the development of the department's internal products.

60 percent of under-35s value the ability to work remotely, but almost two-thirds of cyber breaches are the result of human error

Picture credit: Getty