Morey Haber and **Scott Carlson** explore how changing technology will increase the threat of cyber security breaches over the coming year

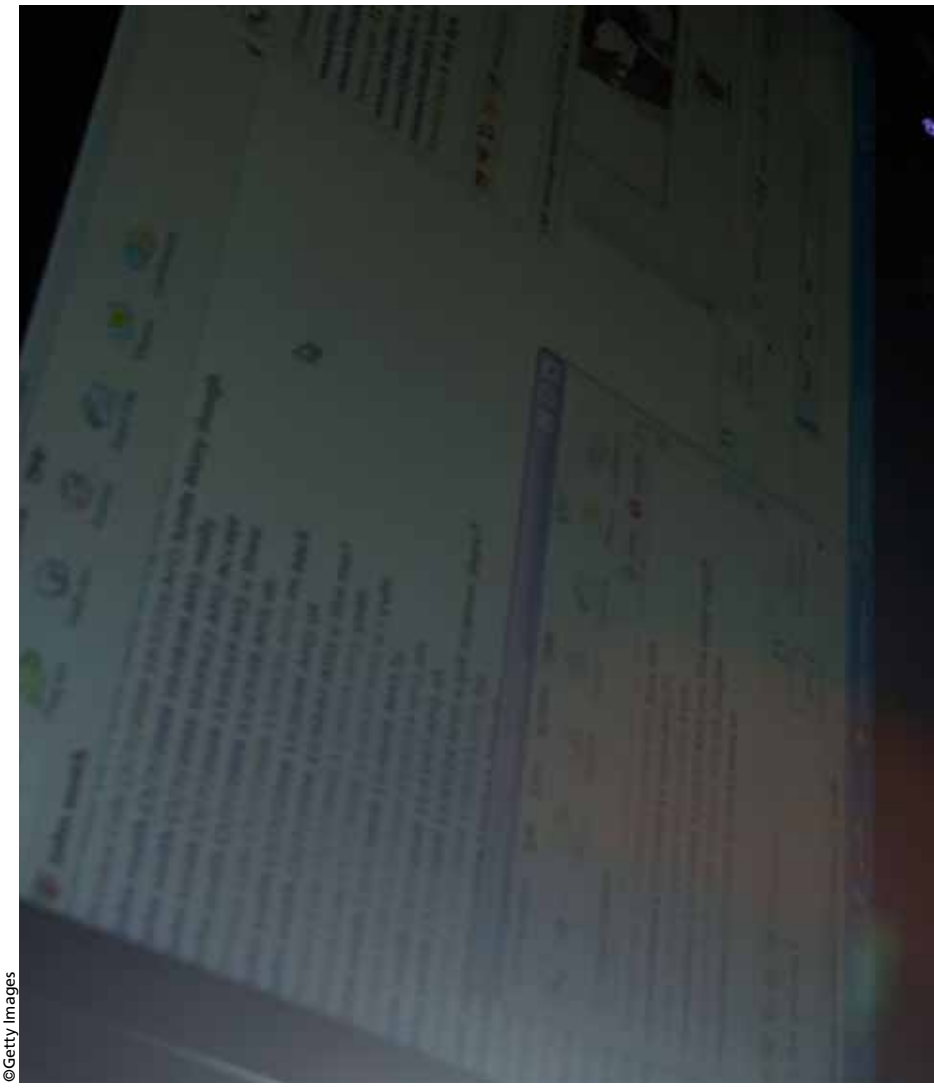
2017 CYBER CRIME SEC

In what has been another story year for cyber security with high-profile incidents such as Tesco Bank and TalkTalk, the start of 2017 is a great time to look at the coming months and prepare. For cyber security, predicting the future is not a purely scientific exercise, but more of an assessment of the past plus an examination of upcoming events with a dash of insight into human nature and the state of the industry itself.

Outside of pure cyber security, the macro trends are also important considerations. As technology evolves from on-premise resources to the cloud, and physical 'dumb' devices start to become more intelligent through the Internet-of-Things (IoT) trend, we enter a time where the digital and the physical are becoming blended and automated within increasingly complex fashions. We are at a point where drones bought from the local gadget store are now potential weapons and governments almost openly perform cyber attacks on each other in an attempt to influence democratic processes. The reality is that if it is connected to the net, it is fair game for an attack. Nothing is immune – from cameras and thermostats, to alarm systems and mobile devices, within refrigerators and toasters. It does not matter who owns them either. Everything from personal systems to voting machines is a valid attack target and, surprisingly, systems not considered worthwhile for an intrusion, become key beach heads for advance cyber attacks. These and other trends make predicting the future for cyber security a difficult yet exciting challenge.

The recent spate of attacks against the fledgling IoT device ecosystem will make the next few years a time when device manufacturers endeavour to improve security. The days of embedded passwords and non-encrypted communication between IoT devices are over. During the near-term, industry groups will start to develop some new standards for communications and encryption on these IoT devices with dynamically generated passwords that require physical access. Other improvements will include patchable firmware/software, secured authentication, and controlled privilege access. If the vendors and industry fail to get up to speed, then it is likely that regulation will be pushed forward for vendor responsibility around IoT device software updates even further than the United States Government has been attempting to pass in recent months.

Today, most IoT devices are considered throwaway items and security patches are not issued. But, new regulations will be driven by large-scale cyber assaults using IoT to amplify the attack. Over the next few years, it is likely that a major hardware manufacture will disclose vulnerabilities that are in the firmware of devices they ship and may be required to do a full-scale recall of the devices. Until then, IoT devices will be released with all sorts of flaws and potential exploit vectors, and many of them will be used to conduct malicious activity.

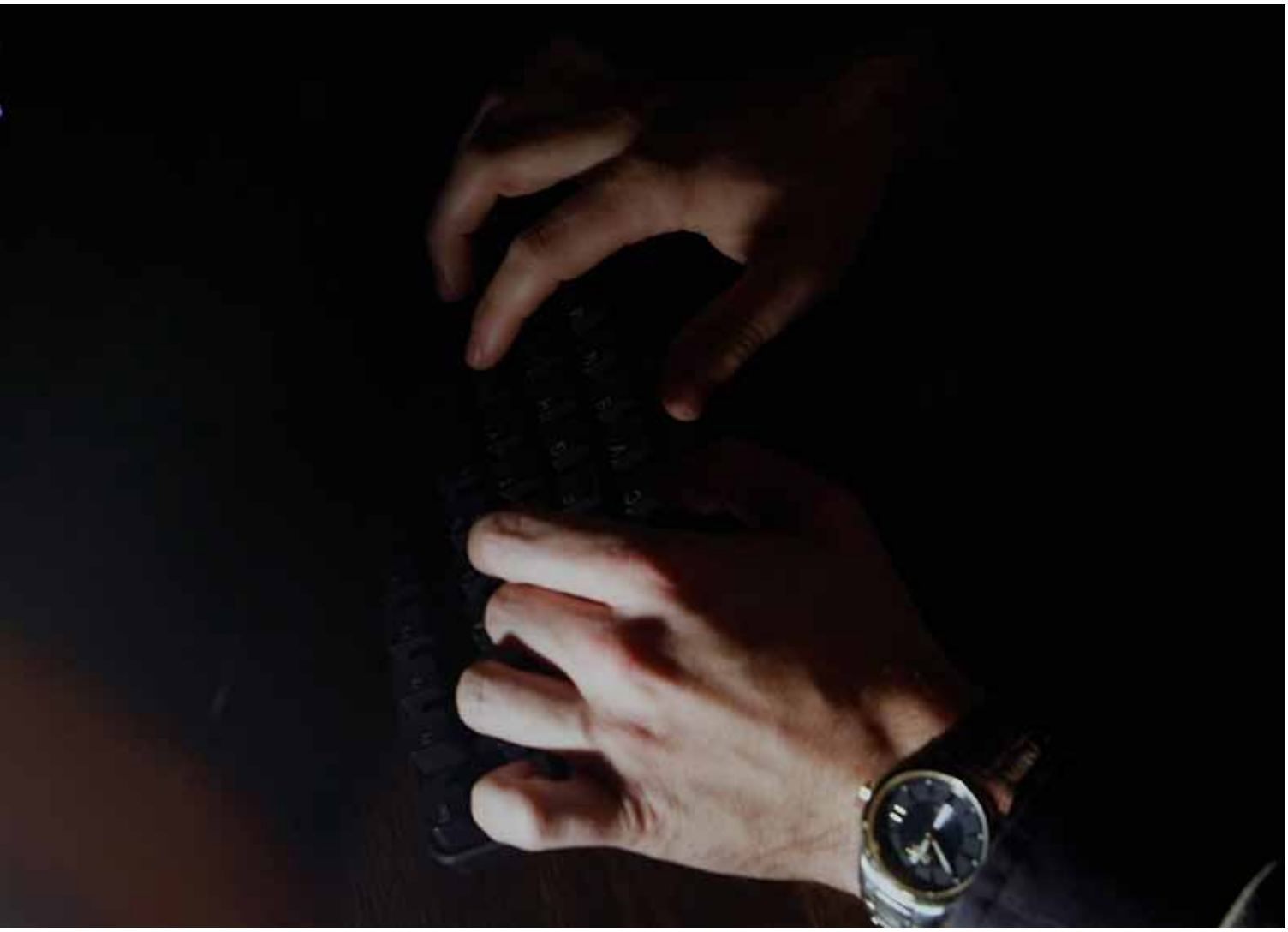


©Getty Images

Yet IoT devices are not alone in this legacy login-name and password approach. Re-using passwords is fundamentally one of the most dangerous habitual cyber security human practices. Large-scale breaches from Yahoo and Twitter will help to fuel the fire until everyone realises the dangers of this practice. It will take a few more major incidents in 2017 to raise awareness. Once this happens, people will begin using unique passwords as often as they lock their car doors in a car park. The next few years will see the rise of more two-factor authentication across not just financial services, but to encompass social, gaming, travel and other areas of life.

In the same way that all ships now have lifeboats because the reality is that boats still sink; the use of encryption is likely to be more heavily mandated across more industries through regulation and consumer pressure. Yet this a double-edged sword for law enforcement as seen by the use of encrypted networks like Tor that have become the conduits for

CURITY PREDICTIONS



international crime and terrorism. The recent tribulations around whether CE device manufacturers like Apple and Google have a moral obligation to make their devices susceptible to decryption with a relevant legal instrument like a search warrant, the near-term future will see more clarity coming from both vendors and governments as to the legal requirements.

Looking out into the future, it is likely that governments will more aggressively infiltrate the Tor network – a position that will force a few large companies to setup cross-country file transfer networks that have terabytes of bandwidth and the equivalent of exit nodes everywhere. This "Tor v2"-type experience will start to be included in most releases of Google software, and will move us toward a network that is fully encrypted and clear-text at all times.

The notion of the impenetrable perimeter is fatally flawed especially against insider threats. The two big issues that need to be addressed are put simply, identity validation and individual intent. The ability to accurately identify that a person logging into an account or making a transaction is really who they claim to be is possibly the single biggest factor in stopping a host of security issues from identity theft to credit card fraud. In the last few years we have seen a rise in federated passwords that allow a login to use a Google or Facebook account to propagate to a whole host of affiliated sites and services. Increasingly, these 'super logins' will have a much more rigid assessment of identity. In the mid-term, a lot more devices will start to release products that have biometric sensors built into the touchpad. This will enable the integration of tools and technologies that advance the concept of biometric/facial recognition into areas like typing speed, pressure and other behavioural-type detection systems. In more instances, these will be mandated for access until it becomes a standard feature for any situation where identity verification is required.

The other side of the coin is intention. Although not quite 'Big Brother', technology that continually monitors each individual's activities will be routinely deployed by both governments and private organisations to intercept security threats. In the same way that credit card companies use algorithms to

2017 CYBER CRIME SECURITY PREDICTIONS

©Getty Images

detect fraud, large-scale data mining and analysis will be in use to find other types of malfeasance. Whether it's an employee copying customer files to pass on to a rival or suspicious sets of purchases from multiple suppliers that suggests a person is making an IED; automated and largely cloud-based security analysis systems will be mainstream within five years.

One of the biggest fears of nation states is an attack that inhibits internet-based services or worse knocks out a large chunk of the internet for an extended period of time. In a worst-case scenario, cyber attacks disrupting power grids or telecommunications could be seen as an attack by a nation, against another sovereign nation, and potentially acknowledged as the first salvo of war. One of the vectors for this type of intervention is denial of service (DoS), which as witnessed can now include millions of mobile smart devices and IoT elements.

With the adage that the best form of defence is attack, it is likely that either nation states or potentially a private company will create systems that directly attacks and patches botnet systems. Almost like a forced inoculation programme, the anti-DDoS service will be directly responsible for patching a hundred million hosts whether they like it or not. Although controversial, the justification could be made for it as a preventative measure to ultimately protect against a mass cyber terrorism attack.

Other forms of cyber counter attack could include the creation of an international internet police force similar to Interpol with WTO/UN oversight to actively interdict criminal gangs that operate internationally via the internet.

Although cyber security is the starting point for many of these predictions, the internet era is fundamentally reshaping how we all deal with identity, access to services and privacy. Within five years, 90 percent of humankind will be online and leaving behind a digital footprint that will allow legitimate and illegitimate analysis to identify almost every facet of an individual's lifestyle, income, employment and even religious and political affiliations. With the scale and scope of data breaches showing no sign of abating alongside the gathering of pools of intelligence about billions of people, within a decade – for a price, all information will be available on almost everyone, everywhere.

In the far future, citizens in countries throughout the world will have to decide about privacy laws because ultimately there will be little information that is truly secret. Many countries will have to move from laws that require non-disclosure of private information to new laws and processes that require alternate factors and validation before any private data is used. Society may shift to a stance where no one cares anymore what is known about the individual, but it is now illegal to use this information to deny benefits, employment, or gain credit. The shift will be from a prevention model to one that is defensive and specific about how, when and where information can be used and will require direct affirmation as to your human identity. This is a major shift and one not dependent on technology, but more on social attitudes.

In a future of self-driving cars, all of these topics come together because no one wants to be in a malware-riddled machine that will kidnap you unless you pay a ransom on the spot.

The growing popularity of the Internet of Things, which includes this smart home temperature control, means there is a far higher cyber security risk

Morey Haber is Vice President of Technology, Office of the CTO at BeyondTrust and joined the company in 2012 as a part of the eEye Digital Security acquisition. He currently overseas strategy for both vulnerability and privileged identity management.

Scott Carlson is Technical Fellow at BeyondTrust, bringing internal technical leadership and strategic guidance to customers, and evangelism to the broader IT security community. He has over 20 years of experience in the banking, education and payment sectors.