What will cyber security look like in the next ten years?

IISP Members and industry experts give us their predictions for the years to come

In 2006 when the IISP was first set up the first iPhone hadn't even been released and the word Cloud just meant a fluffy thing in the sky. In terms of security, most hacks and malware were borne out of someone's back bedroom and designed to annoy, not damage or steal. The infamous Zeus Trojan was still two years away.

Without a doubt over the last 10 years a lot has changed in the security industry and the threat landscape is much wider. Despite certain predictions back in 2006 proving correct, such as threats turning nastier, social networks being taken advantage of, and a drop in traditional bank robberies as cybercrime grows, it is very difficult to accurately predict what is going to happen in such a rapidly changing and evolving technological world. No one predicted the extent to which hacking has gone professional, nor did they predict the total blurring of the lines between personal and digital data, or the need to protect so many connected business and consumer 'things'.

As the IISP's 10th Anniversary year ends, we look at the cyber security landscape and attempt to predict what will change over the next decade. What part will AI be playing in security? What impact will the IoT and ubiquitous connectivity have? Will passwords eventually be replaced in favour of biometric technologies? To help in this quest we have asked IISP members and industry to give us their predictions for the future of the cyber security industry.

Chris Hodson

Chris Hodson discusses mobile botnets, IoT and Ransomware

Mobile Botnets

Cyber-criminals are motivated by making the maximum amount of money through the least amount of effort. As motivation for malware production moved from a kudos-generation tool to a money-making one, the bad guys have always been looking for the widest distribution mechanism for their software. Mobile botnets are an increasing threat. Mobile phones are now pocket computers with added benefit of being able to make calls. We now rely on mobile phones for, amongst other things: email, file sharing, banking, shopping and tweeting.

There was a time when people genuinely believed 'you only need anti-virus if you're running Windows'. Whilst there are esoteric arguments to refute this claim, the feeling was that no one would both writing malware for platforms with a small end-user footprint. From a money-making perspective, they had a point. The premise of a mobile botnet is almost identical to its desktop equivalent: through the distribution of malware, the bad guys want to take complete control of your handset rendering it a botnet 'zombie node'. Once under the control of the bad-guy or 'botnet-herder', the zombie becomes a money-making resource and can be used for anything from data exfiltration, spam email distribution or participate in a Distributed Denial of Service (DDoS) campaign. Botnets are big business for the organised criminal - herds of machines often being rented out for an hourly or daily fee.

IoT

IoT devices are already becoming an increased target and will continue to be so as more-and-more devices become truly connected. And this won't just be for ransomware, but all forms of cyber-attacks, including worms, viruses, and denial of service (DDoS) attacks.

"Unlike vulnerabilities in software, which can be addressed with a simple patch, many hardware products today have no easy means of patching firmware. As such, we're likely to see an entire generation of hardware devices that will simply need to be replaced when critical vulnerabilities are uncovered.

We are seeing an increase in IoT-based botnets because IoT-enabled devices are everywhere and the security development lifecycle for IoT devices is often expedited or bypassed due to strict deadlines around time to market or the cost of the hardware. IoT devices are often, as in the Sucuri case, geographically dispersed

In the case of CCTV, price-point is imperative. The manufacturers are looking for hardware components which are affordable and incrase profit margins. Whereas, in theory, an older version of an operating system can be patched with the latest updates for a vulnerability, what is the process for hardware residing in a CCTV camera? The generally isn't one other than 'replace the hardware' for newer (often more expensive) components. This situation is neither palatable for the consumer or the manufacturer.

Ransomware

One thing is for sure, ransomware is the flavour of the month right now for cybercriminals. The reasons behind this are simple. Ransomware is a high profit and repeatable architecture, almost a malware as a service. The infection methods of this type of malware can include anything from exploit kits to email phishing and with these threats being so real, businesses around the world need to identify the best steps to take to mitigate this ever increasing risk. There is no time to waste, organisations should look to get secure and fast.

With cybercrime establishing itself as a profitable business, the bad guys get greedy quickly and seek to maximise revenue wherever possible. But in order to do this, the criminals need to make sure that their malware payloads evade controls. The most appropriate first step to take is to implement a defence-in-depth architecture. One which contains the ability to provide dynamic and behavioural analysis of malware would certainly suffice and keep the guard up against ransomware. I'd also advise businesses and CIOs in particular, to no longer rely just on signatures.

Rory Alsop
M.Inst.ISP, CRISC, CISM, ISF Executive Council Member

Rory Alsop predicts five problems for CISO's in the next decade

For all the talk of Quantum computers breaking encryption, and API Banks destroying old bricks and mortar banks, I don't really see any revolution in the security landscape over the next ten years, but I do see an ever-accelerating rate of change, and without extra investment and a rethink of security models we will lose out to attackers. Board level is finally beginning to understand Information Security, and with more CISOs gaining a seat at board level with long term security experience much of the impetus (and responsibility) especially in larger organisations will sit with them. I hope they are ready, as their world is only going to get harder. The following 5 areas are the ones I expect to keep me awake at night over the next ten years:

Data Leakage

Despite the GDPR and related guidelines coming into place, my main expectation over the next few years is a ramp up in major Data Loss/Data Leakage events. They get good press and they can be high value to criminals, and in the ever more connected world are becoming harder to prevent. How many partners, suppliers, distributors etc are you sharing data with? Are their defences strong? Are yours? How do you know your "Crown Jewels" are locked up safely? And for those members of staff who have access, how do you stop them taking data out? Disabling CD Writers, USB ports, connections to web mail etc. are all very well, but what's to stop someone printing out a few hundred pages of sensitive data each day and carrying it out in their bag?

Classic attacks

Forget about zero-days and complex new techniques! We will see more attacks through legacy, broken, or known insecure platforms or applications, after all, if a website has an SQLi vulnerability, or uses an old version of WordPress, runs on XP, then it's like leaving the door wide open. Large enterprises will have logistical difficulties doing this because of scale, but really there is no excuse to run old code or kit.

Wetware attacks

Financial Services companies have long had pretty strong perimeter security, both physical and logical, and other industries are beginning to catch up. So with technical controls becoming strong, attackers will once again target the weakest link: humans.

Despite the message all companies pay lip service to, "Don't click links in emails or on websites," we still encourage people to do this every day. And for a well crafted email or web page there is no way for your average person to be able to identify a malicious link.

WHAT WILL CYBER SECURITY LOOK LIKE IN THE NEXT TEN YEARS?

Especially in times of recession or crisis, the cost of bribing or coercing a member of staff, especially low paid, transient staff (such as call centre or cleaning staff) is not high. Simple tasks like placing a keylogger on a PC or a malicious device on a network port can take seconds, and give attackers a route in past all perimeter controls.

Blockchain and other Disruptive tech

Blockchain and crypto-currencies have the ability to change financial services completely, potentially for the better, providing more accurate and verifiable ledger systems, and allowing a greater variety of services and competition to flourish. Unfortunately this also can allow crime the same benefits.

- "Know Your Customer" can become more difficult when we drop the requirement to meet a bank manager.
- Faster payments make tracking fraud much more difficult, especially as the global connected nature of finance has not yet been matched by law enforcement, so some countries are very "friendly" to organised crime groups.
- Implementation of Blockchain solutions is still new and largely untested.
- API's and Open Banking will allow yet more groups access to your data.

There will be mistakes made, and these will be exploited.

DDoS

DDoS attacks have been dramatically increasing in size, and the services offered by DDoS providers range across every network protocol. This will continue as more IoT devices are made without any security, providing ever greater numbers of compromised machines for botnets. Currently there is no requirement for manufacturers to make IoT devices secure - customers don't care and won't pay for it. ISP's also have little reason to prevent DDoS attacks at the upstream end - they aren't negatively affected, and customers won't pay the increased costs required to pay for improvement in this area.

DDoS of IoT may also become a useful tool in the attacker's armoury. Internet-enabled power or central heating controllers will provide the malicious or nosy with information about households, but imagine how effective turning off heat in the winter or air conditioning in a hot summer can be. We have seen both already, but this will escalate beyond the level of inconvenience. In extreme climates, there will be deaths.

So what should we be doing?

Mature organisations have multiple layers of defence, but no layer can be 100% effective. A competent attacker will try to find the holes in each layer and find their way through. As ever, the solution is to make this difficult enough or noisy enough so that an attack can be spotted before it succeeds, but the escalating nature of attack techniques has meant greater investment is required here than ever before.

The controls required are not rocket science, in fact many organisations have much of this already, but the investment required needs to dramatically increase. You will need:

- Strong user access controls to limit the damage that can be caused when an account is compromised
- Internal network segregation, and network access controls that include rogue device detection and device authentication
- Behavioural detection tools to identify malicious behaviour e.g. attempts to connect out to Command and Control servers)
- Get social networking off your business networks! Everyone has Facebook, Twitter etc on their smartphone these days, so removing social networks immediately improves your data loss protection, and removes one avenue of attack, without negatively impacting staff.
- Update and Patch! Move to virtual desktops to make timely updates possible over large enterprise estates.
- Write secure code, rather than try to secure existing code. Developers should all be trained in secure coding practices.
- Thoroughly vet staff, and base the access they are allowed on the risk they present.
- Ensure staff are secure at home - help them secure their home network.
- Provide essential software (eg Microsoft Home User Programme) so staff don't install pirated versions.
- Educate staff on securing their iPad/laptop/phone against their children/grandchildren.
- Require IoT devices to be secure, or at least patchable, otherwise this problem will just grow.
- Require ISP's to filter out DDoS attacks - the services provided by large scale DDoS mitigation providers such as Akamai and Layer 3 are very good, but are protecting at the high volume end. If ISP's were tasked with filtering upstream, the issue would be dramatically reduced. Until this is mandated or profitable for ISP's, however, it will not happen.

CISOs, CSOs and Boards will be under intense pressure from regulators the world over, and this is likely to be a turning point. Make sure you are ahead of the rest, as fines and other punitive costs are going to ramp up rapidly, first around major data leaks, but then around high impact attacks. Otherwise, you may end up being one of the organisations that will lose during the next few years...

Chris Few
Uk Business Manager, Foreseeti

Chris Few looks at Cyber security modelling becoming mainstream

Cyber security modelling becomes mainstream

For decades, many branches of engineering have used computer aided design (CAD) tools to predict the properties of new product designs before they were implemented. But if you wanted a CAD tool to predict whether your IT system design would be secure, you would be disappointed. However, from the rate of progress in this field over the last 5 years, it looks likely that the use of CAD tools for analysing the cyber security of IT systems will become mainstream over the next decade.

In 2013 & 2014 KTH, the Swedish Royal Institute of Technology, published papers on their Cyber Security Modelling Language (CySeMoL). These described its ability to model the key security configuration details of an IT system and to automate the analysis of attack paths through the model. Although time consuming to use, CySeMoL demonstrated a crucial property; it could distinguish between strong and weak security architectures in a way that control based compliance regimes struggle to do. Strong security architectures have no easy attack paths and CySeMoL could exhaustively search through all possible attack paths defined within the model; a task that humans would find laborious even for small IT systems. Its key output, the expected time to compromise, was equivalent to the bottom line on a balance sheet – a simple, meaningful metric that summarised a mass of data.

Today the first commercial implementation of their conceptual model is already available and its developer, Foreseeti, is tipped as one of Sweden's hottest tech start-ups. From this point onwards, market forces and iterative development will drive ever more powerful CAD tools in this field; more powerful in the sense that their models will make more accurate predictions of the most vulnerable attack path, of what attacker capabilities will be required to complete it and how long it will take them to do so. Protocols and data format standards will emerge to automate modelling of existing systems. Actual times to compromise will be compared with predicted times and modelling techniques refined accordingly. Security managers, data owners and regulators will be able to set quantified security targets.

This will bring new opportunities and challenges for the information security profession. Models will still be simplifications of reality. Good cyber security modellers will understand the limitations of their tools and explain the implications to their clients. There will be a need for standards on what a good cyber security model should include and what skills are required to produce one. There will be a demand for training courses and for certification bodies to recognise competent professionals and service providers. But if the cyber security profession can establish these constructs, it can emerge alongside mature engineering disciplines as making quantified, testable predictions of an important system property at the design stage.

Adrian Winckles
Course Leader in Information Security and Forensic Computing

Anglia Ruskin University: 2016 Continuing Year of the Breach, 2017, Year of the Application

It used to be said in terms of security incidents, "there were two types of organisations, those who know they've been breached and those who don't". Increasingly this year we are seeing the former and in the future with GDPR on the horizon we're going to see more and more declarations…

Those of us tasked to protect our organisations data "have to be lucky all the time whilst those who attack only have "to be lucky once". What have we forgotten and what else should we be doing to redress some of the balance to increase our 'luck' in the dawn of everything connected to everything else everywhere?

Organisations have effectively blanket covered much of the infrastructure issues with layers and layers of "swiss cheese" solutions, every solution has potential holes which another solution layer helps to cover. Defence in depth has been deployed as a principle by many organisations but we're still suffering breaches.

We've been told the breaches occur because of zero day vulnerabilities, that are not known about and hence we have protection against. The NSA recently commented that "targets provided attackers with a wide enough vector through poor cyber hygiene".

So what have we forgotten, what have we not considered, so what do we need to think about to make us "lucky" :-

- It's not just about the infrastructure layers
- It's not just about protecting the operating system
- It's not just about what's known (vulnerabilities and exploits)
- It's not just about what not known (zero days)
- Some of its how we use what we've got (poor cyber hygiene)

What's left… The Application(s)

The OWASP Top 10 for Web Application Vulnerabilities was first released in 2003 and over 10 years later many of the vulnerabilities are still a common occurrence in many of the ever increasing breaches being reported. As a community, we've known how to fix the application issues of SQL injection for almost as long as it's been at the number one position in the Top 10 but organisations are continuing to be victims of the vulnerability being exploited.

WHAT WILL CYBER SECURITY LOOK LIKE IN THE NEXT TEN YEARS?

It's not just the applications in use we should be worried about, we've seen plenty of problems with the development environment as well from the likes of vulnerabilities built into open sources libraries for OpenSSL (aka Heartbleed) or entire application development environments cracked and rereleased with malware toolkits incorporated to compromise any application developed (Xcode Ghost). This illustrated the problem can be open source or proprietary environments.

Don't just take my word for it,

- "75% of security breaches happen at the application" (Gartner)
- "Over 70 percent of security vulnerabilities exist at the application layer, not the network layer…" (Gartner)
- "If only 50 percent of software vulnerabilities were removed prior to production…..costs could be reduced by 75 percent" (Gartner)
- "92% of reported vulnerabilities are in the applications not in networks.." (NIST)
- The cost of fixing a bug in the field is $30,000 vs $5000 during coding.." (NIST)

There is a big financial imperative to build security into the application and is certainly going to be the final frontier for security in 2017.

Alan Calder
Executive chairman,
IT Governance

The proliferation of internet connected devices combined with the increasing diversity of platforms and operating systems will continue to complicate the already inadequate efforts of management to secure systems and data. Managements tend to prioritise top line growth, as well as speed and agility in system and product development, which tends to mean that adequate information security measures are most often either an afterthought or simply inadequate. New systems and platforms are not, by default, more secure against evolving cyber threats than were the systems they are replacing.

Software and system evolution will expose more and more unpatched, vulnerable, legacy systems and software in situ in organizations, delivering key parts of critical business processes. In any cases, organizations typically do not know what information they hold, where they hold it, or the circumstances under which it is held. The combination of vulnerable legacy systems and unmapped data holdings is, for many organizations, a data breach waiting to happen.

The number and severity of data breaches will continue increasing, with ever more valuable data being stolen. Data breaches affecting major brands such as Tesco Bank, TalkTalk, Morrison's and even the security solutions provider Verizon Enterprise Solutions are a reminder that cybercrime should be near the top of the board's agenda in every organisation.

A high percentage of successful cyber-attacks now exploit inadequate governance frameworks and untrained staff. A minority go further, and subvert an insider rather than to developing the malware or technology to launch a sophisticated external attack. Organisations cannot simply rely on technology solutions to provide security. Dangerous insiders may be those who seek employment in an organisation with malicious intent and dissatisfied employees who resolve to harm the organisation as well as those whose carelessness or negligence unleashes cyber-Armageddon.

As the insider threat becomes more prevalent, organisations will have to substantially improve how they educate their employees and senior management; there will also need to be ongoing awareness training to ensure everyone stays up-to-date on the tactics, threat mechanisms and methods used by cyber criminals. It is critical that organisations create and embed a cyber security culture to help their employees develop appropriate attitudes and behaviours.

GDPR, and the speed with which data protection laws – increasingly supervised by national regulators armed with significant powers to levy financial penalties – are being adopted around the world will see the domains of cyber security and data protection merge; cyber compliance will become a core part of the role of any CIO or CISO with Data flow mapping as important a cyber security management skill as is the ability to design and deploy an effective patch management process.

HR and Learning teams will also have to become significantly involved in the cyber security strategy; cyber security competencies will have to become a key part of the skill set of many more people within the organisation than presently, and more and more firms will find skills frameworks like the IISP an essential tool for planning and developing their workforces. Alongside the IISP framework, the SFIA is also likely to become increasingly widely known.

While cyber security and data protection are merging into a cyber compliance work strand, cyber incident response and business continuity management are merging into a new discipline called cyber resilience. Those organizations that lead the way in putting cyber compliance and cyber resilience on their board agendas are the organizations that will outcompete their peers over the next five to ten years. Not only does a cyber breach seriously disrupt an organization's normal activities, undermining management and diverting critical resources to recovery, forensic and mitigation activities, reputations are trashed and senior management jobs are lost. More than that, customers desert companies that fail to protect their valuable personal data and, without customers, companies fail.

The future of cyber security is to be at the heart of the business strategy of the world's most successful organizations.

Dr Rob Hegarty
Manchester Metropolitan University

Dr Mohammad Hammoudeh
Manchester Metropolitan University

Future Security Issues

In order to prevent the Internet from being consumed with the challenges of securing the next billion devices. There will likely be a focus on securing the gateways through which insecure, low resource IoT devices gain access to the broader Internet. Recent events such as the Mirai botnet attack on the fabric of the Internet (High Level DNS Servers) illustrate how large numbers of low cost, low resource devices can be corralled by attackers to great effect.

More intelligent routers for home and small business users, could help alleviate this problem. Further steps will be required upstream, in order to negate threats from emanating from legacy devices at customer premises. Collaboration between ISPs and other Internet stakeholders such as Google, Facebook, Microsoft etc. will hopefully become commonplace, in order to ensure the Internet, our worldwide market place from communications and services, remains open for business. AI will undoubtedly play a role in facilitating the analysis of shared data, and prediction of attacks.

It is highly likely that AI will contribute to many security improvements. Unfortunately, it is equally likely that bad actors will leverage AI to develop novel attacks on conventional computer systems and other AI systems. It is also increasingly likely that AI systems will be targeted at they play a greater role in our daily lives.

Our thanks to all contributors for their predictions, we look forward to checking back in 2026 to see how accurate they've been.

And finally, for 2017….

In the shorter term researchers at Intel Security have identified 14 cyber threats to watch in 2017. They are:

1. Ransomware attacks will decrease in volume and effectiveness in the second half of 2017.
2. Windows vulnerability exploits will continue to decline, while those targeting infrastructure software and virtualisation software will increase.
3. Hardware and firmware will be increasingly targeted by sophisticated attackers.
4. Hackers using software running on laptops will attempt "dronejackings" for a variety of criminal or hacktivist purposes.
5. Mobile attacks will combine mobile device locks with credential theft, allowing cyber thieves to access such things as banks accounts and credit cards.
6. IoT malware will open backdoors into the connected home that could go undetected for years.
7. Machine learning will accelerate the proliferation of and increase the sophistication of social engineering attacks.
8. Fake ads and purchased "likes" will continue to proliferate and erode trust.
9. Ad wars will escalate and new techniques used by advertisers to deliver ads will be copied by attackers to boost malware delivery capabilities.
10. Hacktivists will play an important role in exposing privacy issues.
11. Leveraging increased cooperation between law enforcement and industry, law enforcement takedown operations will put a dent in cybercrime.
12. Threat intelligence sharing will make great developmental strides in 2017.
13. Cyber espionage will become as common in the private sector and criminal underworld as it is among nation-states.
14. Physical and cybersecurity industry players will collaborate to harden products against digital threats.