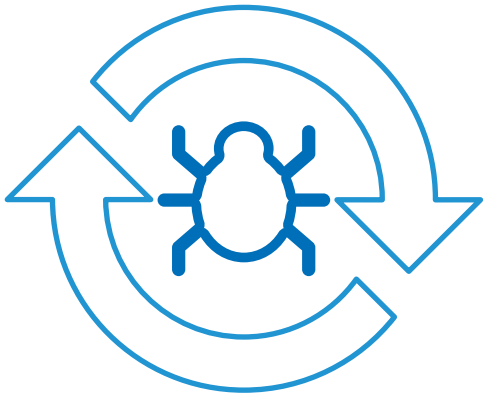
SOPHOS

Security made simple.

Security Threat Trends 2015

Predicting what Cybersecurity will look like in 2015 and beyond

By James Lyne, Global Head of Security Research, Sophos



Cybersecurity in 2015

Cybersecurity is experiencing enormous growth, as an industry and as a theme in the daily lives of people and businesses using technology. And because our technology keeps changing at an astounding rate, threats are evolving fast too – with cybercriminals finding new and creative ways to exploit users and technology all the time.

Now it's the time of year when many parties release their predictions for technology and all of the changes and threats that will come in the next year. Some predictions might be way off in the future, and many are things that are already happening. However, we find it helpful to look at the key trends in cybersecurity, so here are 10 big things we believe will have significant impact in 2015 and beyond.

Exploit mitigations reduce the number of useful vulnerabilities

Cybercriminals over the last few years have taken advantage of exploits to silently deploy their malicious code. In the old days spam was the primary vector of delivery for malicious code but today web based infection and browser based exploits are a clear leader. Fortunately, Microsoft has invested in exploit mitigations such as DEP (data execution prevention, designed to prevent the execution of attacker code in certain parts of a computer's memory), ASLR (address space layout randomization, which makes writing attack code difficult by shuffling memory around), and a huge number of improvements in Windows 8 and Windows 8.1 (a full review of which is beyond the scope of this paper, but which is documented extensively online).

As the difficulty of exploitation increases, exploits in high value target applications such as Internet Explorer on high value platforms such as Windows 7 are becoming more rare and their market value is increasing. We've already seen some behavior changes as a result of this and can predict a few other outcomes. High value exploits are being sold for more targeted use and deployed more selectively, leaving a portion of the cybercrime market with fewer options.

Some attackers are moving back to social engineering rather than using exploits. Be on the look out for more effective social engineering scams as cyber criminals find new innovative payloads. We may also see attackers focusing on non-Microsoft platforms where less mitigations are sometimes present. Consider too that there will be a long tail of users running older platforms for some time (after all, many are still using XP). The new mitigations are driving the value of exploits to even higher prices on the black market, and even greater secrecy in this underground industry. I would be on the look out for more simple and effective social engineering in 2015 and would take a close look at patching strategy and containment processes for non Microsoft devices.

Internet of Things attacks move from proof-of-concept to mainstream risks

In 2014 we've seen more evidence that manufacturers of Internet of Things (IoT) devices have failed to implement basic security standards – either they haven't learned from the long and painful history of failures of mainstream computing or, in their rush to go to market, they just don't care.

I've personally hacked wireless routers with web attacks such as command injection, CCTV cameras that don't bother implementing account lockout, and wireless plugs that don't bother with usernames or passwords and instead explicitly trust the local network. Security conferences have been filled with demonstrations of these issues but as yet it has not translated into widespread interest from cybercriminals. We expect you will see more serious examples outside the proof-of-concept playpen of security researchers soon.

Without better security, attacks on these devices are likely to have nasty real world impact. It is key that the security industry evolves to deal with these devices, that vendors of such applications grow to recognize the importance of security (much as Microsoft once had to), and that consumers continue to grow their awareness of the issue so that it becomes a commercial requirement, not an afterthought or nag from security pros.

Perhaps the reason the Internet of Things has been less exploited so far is cyber criminals have yet to find a business model that enables them to make money. However, as use cases grow more diverse the probability of these emerging grows far greater – and at present trajectory the IoT vendor community won't have buttoned up the security issues before this happens. Worse still, unlike Microsoft that has learned the hard way about patching, these vendors may not even have an infrastructure to distribute updates in a timely fashion.

Encryption becomes standard, but not everyone is happy about it

We predicted in 2013 that full-disk encryption would become a far more common default provided by OS vendors or in hard disks and managed by security vendors – and this trend has largely been realized in the modern enterprise.

With growing awareness of security and privacy concerns due to revelations of intelligence agency spying and newsworthy data breaches, encryption is finally becoming more of a default across the board.

For example, a quick review of mobile applications on Android reveals a significant number of them using encryption to protect data locally on the device and when they connect back to services on the Internet. This number has increased notably from a couple of years ago and seems like reason for celebration.

Unfortunately, while many of these applications have made the effort to use SSL (for example), few of them have implemented this correctly. For example, most do not use certificate pinning, making the encryption more for show than necessarily delivering real security and privacy. In the details lie the difference between effective encryption and "marketing" encryption, but most are auditing for the latter, not the former.

Many more businesses and consumers want to encrypt data flowing in to cloud services from a mobile or PC, but flaws in implementation mean businesses should ask tougher questions than "is it encrypted?". Standards and audit processes will likely be slow to catch on to the details as was the case back in the days when DES was (rather late) deemed inappropriate for use.

Meanwhile, some law enforcement and intelligence agencies are unhappy about this drive for more encryption, under the belief that it will adversely impact safety. While there is undoubtedly a contention between their security goals and privacy keeping everything insecure to allow law enforcement forensics is not a sensible strategy.

There is also an interesting problem for standalone network security providers as more traffic is encrypted and can not be intercepted and scanned at the network. This is likely to have a significant impact on the way security must be delivered in the coming couple of years.

More major flaws in widely-used software that had escaped notice by the security industry over the past 15 years

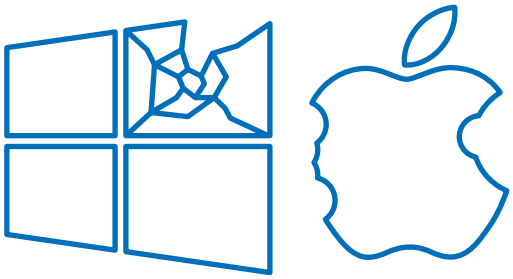
This year saw a number of impactful bugs outside the standard Microsoft platforms that many in the security industry typically have their eyes on. From Heartbleed to Shellshock, it became evident that there are significant pieces of insecure code used in a large number of our computer systems today.

Many were alarmed to find out that the OpenSSL project (widely used software integrated in to more places than you could imagine) didn't have the resources to do proper audits and code checks a lot of the time, despite being incredibly widely used.

Many of these defects may not reach the same severity as the ones we saw in 2014, but they represent an interesting challenge for businesses none the less. Enterprises have developed and practiced protocols for deploying patches or managing risks on Windows systems, but many have nothing like this for other platforms. This was evident in the very slow patch times of many businesses trying to respond to Heartbleed. Sadly even now there are many brands that are vulnerable months after the flaw made international news headlines.

Unfortunately, I don't feel confident these lessons have been learned and further vulnerability discovery in non-Microsoft systems will lead to long periods of exposure for large numbers of users.

The events of 2014 have boosted the cybercriminals' interest in typically less-considered software and systems for the years to come – so you should be preparing your response strategy for those areas too. This will challenge many of the processes and procedures businesses have in place.



Regulatory landscape forces greater disclosure and liability, particularly in Europe

The law moves slowly compared to the technology and security fields, but massive regulatory changes that have been a long time coming are very nearly here. After years of talking about mandatory breach disclosure, data protection officers, and hefty fines, the European Union is on the cusp of implementing tough new standards in 2015, with enforcement commencing in 2016.*

In recent surveys in Europe, we've found that the majority of businesses have no idea this is coming, even though failure to protect data could result in punitive fines up to €100 million or 5% of annual revenue. A staggering 77% of the surveyed businesses didn't even know if they were compliant with present data protection regulations, let alone the upcoming ones. It is likely these changes will also trigger consideration of more progressive data protection regulation in other jurisdictions.

There are significant challenges with cybercrime laws, ostensibly still national in their implementation when cybercrime is an international issue. I expect there will be more complaints about the limitations and appropriateness of national laws such as the Computer Fraud and Abuse Act (CFAA) in the U.S., and similar laws around the world. But a more international approach is not forthcoming at this point.

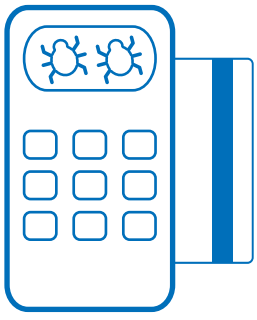
***This being a draft regulation means timeframes and scope are subject to change, though it is looking very likely to make it through the process and be implemented as described.**

Attackers increase focus on mobile payment systems, but stick more to traditional payment fraud for a while

Mobile payment systems were the talk of 2014 after Apple stormed ahead with Apple Pay. Undoubtedly there will be implementation mistakes in these new protocols, but the initial forays by Apple seem to provide greater convenience and improve upon the security standards of many of the world's credit or debit cards, particularly the U.S., which sticks to rather archaic and fraud prone standards.

Cybercriminals will be looking for flaws in these systems, but the present designs have several positive security feaures: special hardware that makes it much harder to extract information; the use of a PIN, password or fingerprint for authentication (much stronger than a signature); and a token to represent your authorization (meaning hackers can't steal the equivalent of a credit card number to use again and again even if they break into the payment wallet).

It is clear that these payment systems are an improvement over simple, easy to clone cards. Breaches such as Target demonstrate the major weaknesses of the present schemes in use in America. New payment systems will more resistant to theft. Expect cybercriminals to continue abusing traditional credit and debit cards for a significant period of time as they are the easier target for now. Watch this space for flaws with new systems as cyber criminals find innovative ways to profit.



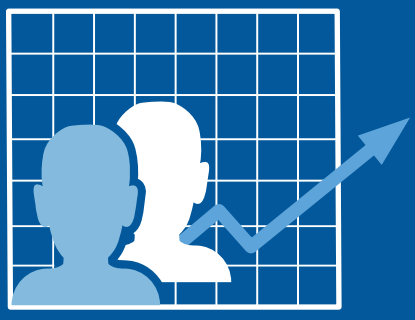
Global skills gap continues to increase, with incident response and education a key focus

More and more data breaches and attacks are making the news, a trend that is likely to grow as mandatory disclosure becomes more common and organizations have to own up publicly to their mistakes.

As technology becomes more integrated in our daily lives and a supporting pillar of the global economy, the cybersecurity skills shortage is becoming more critical and broadly recognized by governments and industry.

This gap is growing larger rather than smaller with some governments forecasting that they will need until 2030 to meet the present demand for security professionals. Combine this with the flow of breaches and the requirement to handle incidents when they occur and there is a competitive scrabble for security professionals.

Businesses should consider their recruitment strategy for these professionals and the industry as a whole needs to make it clear to graduates that there are career prospects in this exciting space.



Attack services and exploit kits arise for mobile (and other) platforms

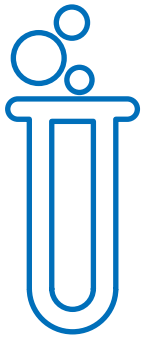
The last few years of cybercrime have been hallmarked by the rise of products and services to make hacking and exploitation point-and-click easy. Some of these crime packs have extended their capabilities to mobile, but none in a major and focused way.

With mobile platforms being so popular (and increasingly holding juicy data too) I suspect it won't be long until we see more crime packs and tools focusing on these devices explicitly. We may also see this trend come to fruition for other platforms in the IoT space as these devices proliferate around us.

At the moment the majority of malware for non-Windows platforms is targeted at Android, with the vast majority of it posing as legitimate applications and tricking the user into installing their nasty code. This trend will continue undoubtedly continue, but the ecosystem for validated application delivery is growing tighter, making side loading of applications a little more challenging for the crooks. This may in turn lead to focus on exploit development for these platforms and the development of exploit kits to commercialize the capability and make it simple.

Note later versions of mobile software have ASLR (userland and Kernel) and sandboxing features (amongst other security controls). While these platforms are far from perfect and many users are running older versions without said enhancements , but automatic updating is becoming a more frequent default. This makes targeting these platforms more difficult and the volume of exploits is much lower than web browser-based exploitation of the PC.

We will undoubtedly see continued focus on mobile devices and I expect the next couple of years to bring new innovation from the cybercriminals in commercializing non-PC hacking, with a mature threat model.



The gap between ICS/SCADA and real world security only grows bigger

Industrial control systems (ICS) are typically 10 years or more behind the mainstream desktop environment in terms of security. It is not uncommon when reviewing these platforms to find a lack of authentication, encryption or integrity-checking where the only viable security strategy is to keep them isolated on air gapped networks.

Unfortunately, on many occasions these systems have ended up inadvertently connected to outside networks – it only takes a quick scan with tools like Shodan to find a surprising number of control systems connected to the Internet. Fortunately, there haven't been too many serious incidents so far.

The reality is that many of these devices and vendors are accustomed to a set of criteria focused on resilience or control and have not learned to speak the language of security that other technology fields had to absorb. They have also relied heavily on isolation and an air gap to prevent attack.

While there are security initiatives from the bigger players in this space, the gap between the mainstream world of security and ICS is only growing bigger. Over the next couple of years I anticipate we will see a number of far more serious flaws exposed and used by attackers as motives continue to evolve from being by majority financially motivated. I expect this will drive greater regulation and industry standardization in these areas, but that it will take a long time to change given their high cost, high complexity and often bespoke nature. In short, it is an area where I feel many are at significant risk and security is less on the agenda than outsiders would expect.

Interesting rootkit and bot capabilities may turn up new attack vectors

Many of the attacks over the past few years have been at the application layer (even DDoS attacks were substantially focused on the application layer rather than the transport layer). Many of the major protocols such as IPv4 have been in production use for some time and we have grown used to their inadequacies and design oversights. However, we are at the cusp of a significant period of change. A whole new version of HTTP (2.0 the successor to 1.1) is on the way and IPv6 has slipped in to widespread use in networks without most administrators noticing.

We are in the process of changing major platforms and protocols from those that we have relied on for some time and these lower level changes will likely bring interesting flaws that cybercriminals may be able to capitalize on. There are a huge number of areas that this could apply to, but consider we've already seen some signs of this. The IPv6 stack on Windows 7 and Windows 8 is vulnerable to a resource exhaustion flaw which allows an attacker to send continuous random router advertisements and consume 100% CPU of the system (until Microsoft partially patched the problem they could crash the system entirely) and most people don't even know the flaws is present, despite still being effective even today.

More broadly, IPv6 re-implements some of the old trust flaws of IPv4, such as providing mechanisms to do man in the middle like with ARP poisoning in IPv4. While there are provisions in the standard to deal with this they aren't yet making it in to real world implementation and policy.

Consider also the lower level hardware changes being made such as the shift to UEFI. UEFI provides a rich boot environment that is significantly easier to program than with a traditional BIOS. The rich boot environment provides interesting rootkit and bot capabilities that may turn up new attack vectors or more powerful versions of attacks we have not seen for some time.

Overall it seems that we are set to repeat many of the mistakes we made the first time when deploying such technologies and we are on the edge of a mass of major changes to the old guard technology standards. Watch this space for old wounds re-opened or major new security flaw categories.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK | Boston, USA

12.14RG.na.simple

SOPHOS