Integrity360
your security in mind

2016: The Year Ahead

Sean Rooney
Cyber Risk & Assurance Director

December 2015

Sean Rooney
Cyber Risk & Assurance Director

I wonder if somewhere out there, cybercriminals are looking back at the year and taking stock of what was most profitable for them and planning the year ahead based on that analysis. It's one of our tasks as security professionals, especially at this time of year, to attempt to predict what those plans might be.

Looking back at the activities of the year just gone, there are new patterns of criminal activity emerging, and some twists on old activities. We have seen an increase in online extortion, an increase in breaches via the supply chain, and an increase in financial fraud with well researched targeted phishing campaigns at senior executives and finance departments.

Ransomware has been prevalent and high profile breaches continue to make the headlines. Breaches are becoming so commonplace, that they often don't make the headlines anymore unless they are very high profile with significant customer data affected like the Ashley-Madison and Talk Talk breaches.

What does all of this mean for the year ahead? Instead of writing this in terms of predictions, which has the connotation of something that may or may not happen, I am writing this as what we need to do about these things that are just a logical continuation of an existing pattern. This is what I believe is going to happen in the months and years ahead. What we need to do is ask ourselves are we doing enough to meet this head on and what more can we do?

Detection & Response

Let's look first at Ransomware. That's going to continue to grow because of its opportunistic nature and likely to be successful, especially for smaller businesses who aren't ready for it. Here, as in nearly all areas we need to focus our efforts on resiliency – how are we going to be able to bounce back fast when a breach happens? It is now accepted that breaches will happen, it's just a matter of time. We need to be ready to deal with them with a well-rehearsed plan. Best case scenario is catching them before any loss or damage occurs, but if we don't manage that, we need to be able to recover quickly. To catch them quickly we need to continue increasing our efforts in the "detect" space.

Earlier this year Verizon released their report emphasising that the length of time taken to identify compromise is still too long. They highlight the "detection deficit" between attackers and defenders as one of the primary challenges in the industry currently. While we're doing a lot more to develop our skills and protect ourselves as individuals, companies and even nation states, the other side of the coin is that so too have the criminals developed their skills and savvy and continue to find new ways to exploit and cover their tracks.

Supply chain compromise

Attacks through the supply chain are continuing to increase and this is an area we need to increase our focus on. There are two sides to this coin – the client and the supplier - and this is regardless of size, no business is immune. As clients we need to know how suppliers with access to our systems and data manage their security. As suppliers we need to make sure we are doing everything we can to ensure we are operating in a secure way. We need to be able to provide the necessary levels of assurance to our clients.

Industry research shows that many organisations are seeing the benefits from adopting Risk Based Cyber Security Frameworks and as suppliers, this is a good place to begin. Such frameworks include ISO 27001, NIST and the Ten Steps to Cyber Security that has been adopted by the UK in its Cyber Essentials program is also a very good place to start.

EU data protection legislation will begin to take further shape in 2016 and while the proposed legislation does not require specific types of technical controls to be in place, companies are recommended to implement a proactive approach to security.

People Vs Technology

Attacks on the people in our teams will continue unabated; targeted phishing campaigns, exploitation, extortion and fraud will be the order of the day unless we begin to do something about it. People will continue to be the biggest risk in the protection of data. There is technology available, if not already in place, and processes keep improving however the human element remains weak. Overload of information, ease of access and ease of use are all factors that can lead to accidental actions that lead to breaches/incidents.

Link this with the shortage of experts to defend and promote secure practices will increase the risk environment. Engendering a sense of relaxed awareness in our people, like we have when we are driving, is what is necessary for us to strengthen our defences through our people.

To do this we can begin to move away from compliance based user awareness training to a program that promotes awareness and more importantly, brings about change. Keeping on the topic of people, skills shortages for security services will continue to be a strain and companies will need to look in different career streams to entice people into the security career path.

Boardroom Focus

Security discussions are becoming commonplace in the boardrooms with many CIOs naming security as their top priority. This is positive in one respect as getting executive buy in is crucial for the success of many security programs, while overall it is worrying because it means that the risk is increasing and so needs attention at this level.

This trend will continue through 2016 and beyond, with security becoming increasingly on the business agenda rather than being the sole responsibility of the IT department. Where there once were almost conflicting interests when it came to security it will gradually come to be seen as an enabler for businesses, helping with operational effectiveness instead of restricting it.

The move to the cloud will continue as trust increases and as a result we will see more cloud based security offerings from security vendors. Security technologies are being developed and adapted specifically for the cloud and this trend will continue. Microsegmentation will enhance security in our datacentre environments dividing the environment into smaller protected zones, rather than just focussing on the security of the perimeter. The security of the "Internet of Things" has already shown weaknesses and depending on the device, could mean that the Confidentiality, Integrity and Availability model will have to be updated to include Safety as a major concern for security professionals. On demand and adaptive security will become terms we hear more and more about in 2016.

In the world in general, the growing unsettled nature of the mid-east region of the world may bring attacks on critical infrastructure and key commerce, such as banks, stock exchanges and any organisations that support western society.

Security is no longer niche; it must become pervasive in our thoughts and actions – in everything we do.

About the Author

Sean Rooney

Cyber Risk & Assurance Director

With over 16 years' experience, Sean plays an integral part in Integrity360's strategic direction and development. Having implemented key solutions for some of the largest corporates in Ireland & the UK, Sean has a thorough understanding of the practical implications and conceptual effects of ICT security policy and procedures. His certifications include GIAC GSEC, GCED and GSNA. He is widely regarded as one of the most competent ICT Security Specialists in the industry.

Integrity360

your **security** in mind

Managed Security

Technology Solutions

Incident Handling

Security Testing

Security Integration

Governance, Risk & Compliance

Integrity360

your **security** in mind

DUBLIN	LONDON	GLASGOW
+353 1 293 4027	+44 203 397 3414	+44 141 255 1925

www.integrity360.com