

CYBER SECURITY AND CLOUD TRENDS

FOR 2020 AND BEYOND

BOOST
TECHNOLOGY GROUP



INTRODUCTION

The pace of cyber security breaches is growing at an exponential rate. Alongside this, the type and variety of cyber-attacks and breaches are growing in sophistication. Organisations always need to be one step ahead to counter the growing cyber threat.

The advances and procedures set up to counteract the growing cyber threat also needs to grow and adapt, and one thing is clear, the top threats in the next few years will be different kinds of threats known to cyber security experts today.

Through 2020 and beyond, 99% of vulnerabilities exploited will be ones known to IT and security experts for at least a year. Organisations must keep focused to fix the vulnerabilities that they know exist to protect their customers. Sometimes these can be barely noticeable, but they can be simpler to exploit and cheaper to fix than to mitigate.

In a world of digital transformation, cyber security is still a hot topic. It should also be a top priority for organisations in all kinds of industries because of the huge amounts of data they create every day. The responsibility of keeping networks secure, taking measures to protect data against cyber threats and ensuring the safety of data they hold has become even more crucial than ever.

Cyber criminals have become even more sophisticated in their attempts to gain access into key systems and many on the C-suite predict that cyber security will become right at the top of their agenda in the coming years.

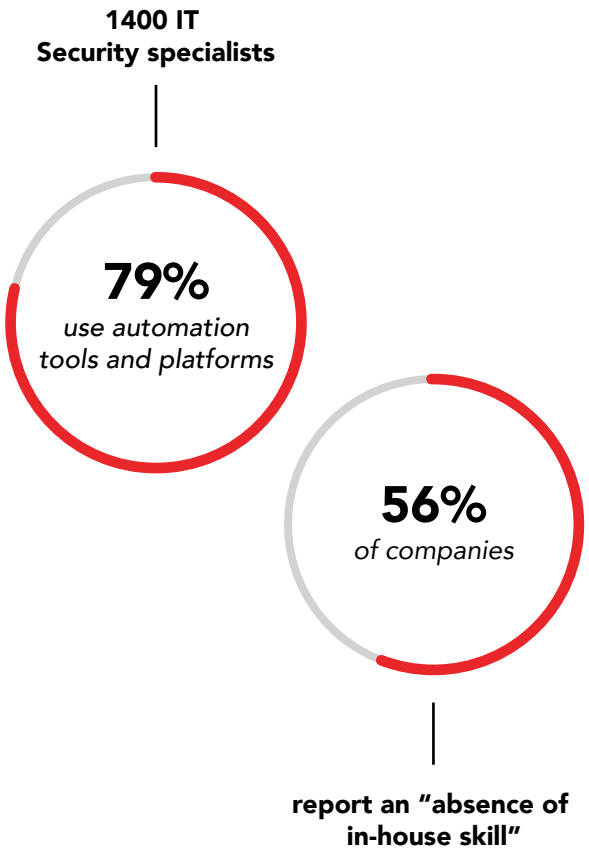
At Boost Technology Group we help organisations in the cyber security and cloud space generate more demand for their existing products and services. Through our award-winning work we come across new cyber security threats and data breaches, which are growing daily.

We've put together ten of our top predictions in the cyber security and cloud space for 2020 and beyond.

01. AN INCREASE IN AUTOMATION IN CYBER SECURITY

Automation is gaining a significant advantage in cloud and cyber security. According to a recent study conducted by the Ponemon Institute of more than 1400 IT Security specialists, 79% of respondents use automation tools and platforms inside their company or plan to utilise them within the next couple of years.

This development towards organisations utilising automation is in the hope of decreasing the burden on understaffed cyber security teams and ensure effectiveness in those teams. However, it is not an ideal solution because automation tools require skilled and knowledgeable people to operate and run them – 56% of companies report an "absence of in-house skill" to help automation be adopted successfully.



02. CYBER SECURITY AND CLOUD SPENDING WILL INCREASE AS ORGANISATIONS LOOK TO DO MORE TO PROTECT THEMSELVES AGAINST THE GROWING CYBER THREAT

Cyber security and Cloud spending is increasing at an exponential rate. Worldwide spending on cyber security solutions such as hardware, software and services is predicted to top £103 billion in 2020. This is an increment of 9.4% more than 2018.

This pace of development is likely to be seen for many years to come as businesses and organisations put their resources into security solutions after having a "head in the sand" approach to cyber security. In 2020 the C-suite will start to take cyber security more seriously and this in turn will have an impact on the amount that is spent in this area.

"WORLDWIDE SPENDING ON CYBER SECURITY SOLUTIONS... PREDICTED TO TOP £103 BILLION IN 2020. THIS IS AN INCREMENT OF 9.4% MORE THAN 2018."



03. THE USE OF ARTIFICIAL INTELLIGENCE WILL INCREASE TO HELP DEFEND AGAINST ATTACKS, BUT ON THE FLIP SIDE THERE IS LIKELY TO BE AN INCREASE IN AI BEING RESPONSIBLE FOR CYBER-ATTACKS

Attackers in 2020 will be likely to use AI strategies themselves to boost their criminal activities and won't simply target AI systems. Automated systems controlled by AI could potentially test networks and systems for vulnerabilities that are not familiar and are likely to be exploited.

For example, Artificial Intelligence could be used to make phishing and other social engineering attacks appear more sophisticated by making them with credible video and sound to create emails that are intended to trick those who are targeted by them. AI could also be used to launch disinformation attacks and help with the spread of "fake news".

However, threat identification systems today use machine learning techniques to detect new threats. In addition, it isn't just attackers that can utilise AI frameworks to probe for vulnerabilities. AI can also be utilised to protect itself from attacks. For example, AI controlled systems could dispatch a range of simulated attacks on an enterprise level system after some time with the full expectation that an attack of this nature will uncover a vulnerability that can be closed off before it is found by attackers.



04. THE GROWTH OF 5G MAY LEAD TO MORE CYBER-ATTACKS

5G is now here to stay, and with various network infrastructure developments taking place in the UK the growth of this new technology will have an impact on the amount of cyber-attacks we will see in 2020.

More 5G enabled "internet of things" gadgets will connect directly to the 5G network instead of via a Wi-Fi router. This pattern will render those gadgets to be defenceless eventually against a direct cyber-attack. Also, the ability to back-up or transmit huge volumes of data effectively to cloud based storage will give attackers new targets to be breached.

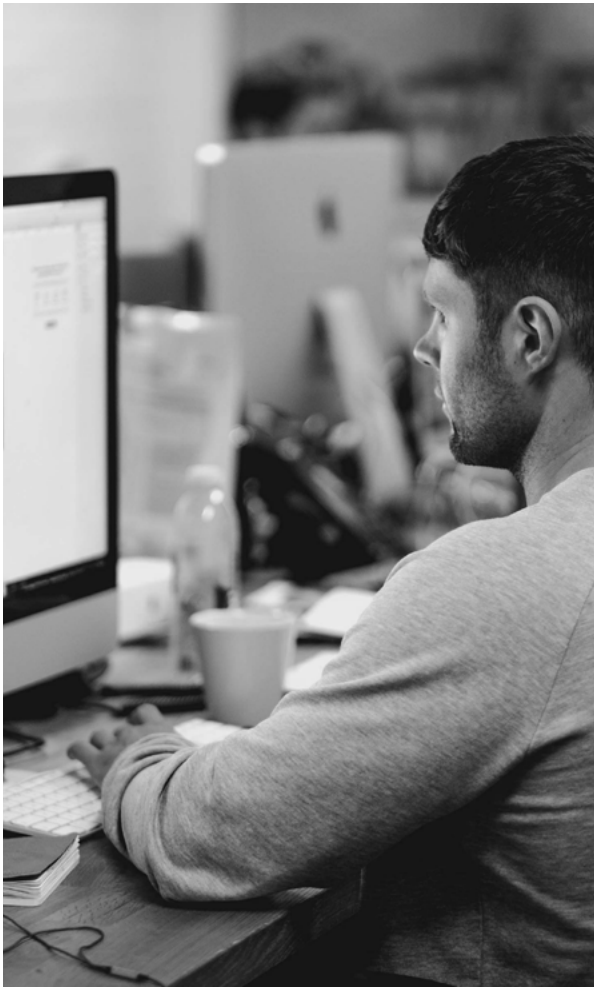
As soon as 5G networks are rolled out to all, devices will be powered on and connected from a wide variety of mediums, and if they are not secured this will increase the cyber security risk of them being attacked exponentially. Everything from business security cameras to industrial-grade smart sensors will be able to tap into the 5G higher performance network. This in turn will provide attackers with a whole new range of devices, tools and systems that they can use to their advantage. With these new devices being introduced to the 5G network, the security landscape will become broader.

Security solutions will also need to be upgraded to deal with the new capability of 5G, especially when it comes to monitoring, encryption and prevention, as the latter is handled by firewalls. Many legacy solutions may no longer work on 5G because of the higher capacity, speeds and latency that 5G provides.

05. THE SUPPLY CHAIN IS LIKELY TO BE EVEN MORE OF A WEAK LINK TO ALLOW CYBER-ATTACKS TO TAKE PLACE

A regular area where cyber-attacks are rife is the software supply chain. Attackers will often embed malware into software bundles when they are distributed.

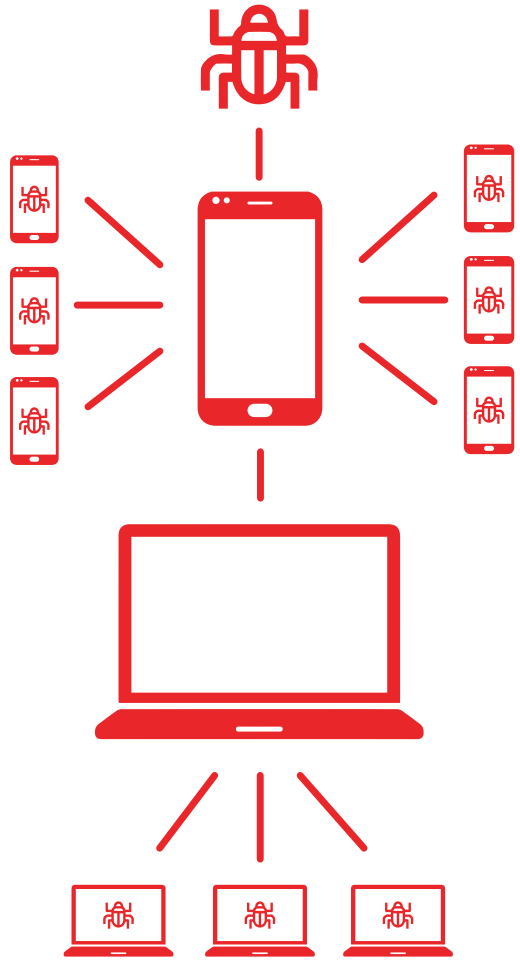
These attacks could happen when the software is made directly by the vendor, or via a third-party software provider. This kind of attack simulation could include the attacker planting a genuine programming update with some malicious code embedded into it which allows it to be spread rapidly to its intended targets. Any user could then potentially accept the software update and have their computer or devices affected.



06. MOBILES AND OTHER DEVICES WILL BECOME MORE OF AN ATTACK VECTOR

Even if organisations issue their employees with locked-down smartphones and devices, embracing best practice when it comes to security remains critical. Cyber criminals are wise to this and have been seeking out and exploiting new attack vectors out of our obsession with smartphones.

In 2020 and beyond the mobile threat landscape will become much more vulnerable as mobile services and smartphones rapidly expand and contain new features and apps. Attacks are likely to be delivered using malware and selfie-style apps like FaceApp, and security for these apps needs to be paramount.



07. LOCAL AND NATIONAL GOVERNMENT INFRASTRUCTURES WILL BECOME MORE OF A TARGET

Local and National Governments today face pressure from all sides, and IT departments are forced to deliver more but with less budget. Indeed, the advent of the "WannaCry" cyber attack on the NHS showed just how woefully inadequate and antiquated their IT system infrastructure is, with much of it still running on Windows XP.

On the one hand, the general public are demanding more and more in terms of digital services and simple online experiences from local and national governments. On the other, government leaders are reluctant to put budget into delivering this. Doing more with a very limited budget in the public sector is today's reality.

Local and National Governments hold huge amounts of data, and as such cyber criminals are aware of this and ready to exploit the value of that data. They will often sell the data they obtain on the dark web or through extortion tactics such as ransomware attacks.

If Government departments expand their technology infrastructures it tends to be at a rapid pace to match the number of services they offer online. In 2020 these departments will be subjected to a much bigger infrastructure complexity, with many local and national governments offering services via mobile or web apps. Simpler security solutions will be called for in order for Local and National Governments to continue their digital transformation activities without compromising on their security.



08. CYBER-ATTACKS ON THE CNI (CRITICAL NATIONAL INFRASTRUCTURE) WILL CONTINUE TO INCREASE

The Critical National Infrastructure (CNI) has always been under the threat of a cyber-attack, but in 2020 this threat is likely to increase ten-fold. It is entirely possible that a global ransomware attack could shut down the entire electrical grid in the UK. In 2020 a cyber-attack on the CNI in the UK is likely to be a matter of when, not if.

The repercussions of the "WannaCry" attack in 2017 which greatly affected the NHS as well as other emergency service provisions and manufacturing plants all over the world are still being felt today. It made many critical services grind to a total halt. With the increasing use of technology within the CNI the industry is under more pressure than ever to keep data secure while in transit.

In an attempt to combat this in 2020 cyber security solutions will be layered to patch network vulnerabilities to keep data secure. Encryption management will also be a must, with many CNI organisations needing to have a robust solution that focuses on protecting data rather than the network it is transmitted on itself.



"IN 2020 A CYBER-ATTACK ON THE CNI IN THE UK IS LIKELY TO BE A MATTER OF WHEN, NOT IF."

09. THE PHISHING LANDSCAPE WILL EVOLVE, AND PHISHING EMAILS/ATTACKS WILL BECOME MUCH MORE SOPHISTICATED

Phishing has already posed a serious threat to organisations of all sizes across the globe, and in 2020 that risk is likely to increase. Most people believe they would be able to successfully identify a phishing email, but cyber criminals are staying one step ahead and coming up with new ways for phishing emails or messages to evade being detected. New phishing scams appear every week and in 2020 we will see more trickery with malicious attachments, compromised credentials, fake cloud storage links, spoofed websites and malicious URL's.

These attacks are highly targeted and cyber criminals will use an extensive range of social engineering techniques to research and study their victims, how they think and what makes them tick to ensure as much success as possible when deploying a phishing email or message scam. Once they have got hold of all the information they need, attackers will even try to impersonate a trusted friend or colleague and attempt to get hold of sensitive information from them via email. If organisations are to successfully defend themselves against phishing attacks, they will need to up their game considerably in 2020. All the technological advances in this area in the world will be worthless if just one employee clicks on a malicious link. The sad reality is that it will be as easy and as destructive to an organisation as that, and one small lapse in judgement by just one employee will bring an organisation down completely.

10. MORE PRIVACY CONCERNS MEANS MORE NEED FOR CYBER SECURITY AND CLOUD REGULATION

The implementation of GDPR and other global privacy regulations has shown that in 2020 there will be an even greater sense of urgency around how organisations manage their cyber risk. It can no longer be passed off to a company's IT department and will be a pressing issue in the boardroom and for the C-suite to deal with. It will also require strong leadership, decisive action and an ongoing commitment to data protection.

Cyber security and Cloud organisations must take into account this need for greater concern around privacy and regulation and take all appropriate security measures to protect the personal data they process or face significant financial losses. Fines that have been imposed by the ICO can be great, and these are likely to be bigger than ever in 2020 and beyond. The consequences of non-compliance will be huge in the coming years.



FINAL THOUGHTS

Although we don't have hindsight to show exactly what cyber threats will be faced in 2020, our guide will hopefully give organisations some insights into the current threat landscape and get them thinking about what they can do to protect themselves from a cyber-attack.

Today's always-connected world creates far more opportunities for cyber criminals and every IT environment, large or small, is a potential target for attack. This includes IoT devices, mobile devices, cloud and on-premise networks. Forewarned is forearmed – **by using threat intelligence to their advantage, businesses of all sizes can automatically protect themselves against upcoming cyber-attacks.**

ABOUT |
BOOST TECHNOLOGY GROUP

Boost Technology Group is an award-winning channel-services provider that helps cyber and cloud businesses improve their chances of winning business through the provision of specialist marketing, sales education and sales enablement services.

With the cyber security and cloud industry experiencing exponential market growth of more than 30x in the last 13 years, we can help you be part of that growth and generate more demand for your existing cyber security and cloud products and services.

As our finger is always on the pulse of all the latest data breaches, trends and developments our dedicated marketing experts can help you stay one step ahead of your competitors to enable you to win more business.

If your cyber and cloud business needs a boost, we can help.



JOIN THE REVOLUTION.

CONTACT US AND BOOK
A **FREE** DISCOVERY
CALL TODAY.

BOOST
TECHNOLOGY GROUP

Boost Technology Group
26 Dover Street, London W1S 4LY

0203 740 4074
contactme@boost-performance.co.uk
www.boost-performance.co.uk