How we stay ahead of a changing threat landscape

Attributed to BT Group

### **The security threat landscape is confusing and changing rapidly – there’s so much out there, how do you understand where the true risks are?**

Every [40 seconds](https://www.forbes.com/sites/forbestechcouncil/2017/09/21/what-it-means-to-have-a-culture-of-cybersecurity/#189651c4efd1) a business falls victim to a ransomware attack. Cyber criminals are creating an average of around [1.4 million phishing websites every month](http://www.zdnet.com/article/1-4-million-phishing-websites-are-created-every-month-heres-who-the-scammers-are-pretending-to-be/) with fake pages designed to mimic the company they’re spoofing.  At BT alone, we detect more than 100,000 malware samples every day — more than one a second. But [99 per cent of malware is used for less than one minute](https://www.verizonenterprise.com/verizon-insights-lab/dbir/). In addition to over 4,000 cyber-attacks, daily, BT and its customers see three million suspect emails per month.

In this article, we talk to the team protecting BT about how we're responding to the changing threat landscape and how you can apply the learnings to your organisation.

## **A security breach is inevitable**

It’s difficult to admit, but no system is 100 per cent secure. We all need to face the fact that at some point, we will be breached.

We’ve observed an acceleration in the production of new attacks, especially those that regularly evolve to evade security controls which can’t keep up. For example, the Emotet malware changed the links or attachments being used to deliver the virus up to 24 times a day. Automated tools have made it easy for criminals to launch attacks, making this new environment a more difficult one for security teams to operate in successfully.

That’s why security has to be a part of your strategy that’s always evolving. As threats shift and your needs change, your security strategy needs to change too.

## **Threat intelligence to stay one step ahead**

Because of BT's global scale, client base, and active relationships with leading law enforcement and cyber security authorities such as Interpol, Europol and the UK National Cyber Security Centre, we’re often the first to correlate events and know of new attacks. For example, we were able to give our customers intelligence around Wannacry six weeks in advance.

Security teams can be overwhelmed by the volume of data being picked up by a raft of security monitoring tools which are not correlated to provide intelligence that is easy for analysts to understand and act upon. Integration and automation are key to keeping pace with the changing threats.

But a tool is nothing without the analyst sat in front of it. By drawing out abnormalities, analysts can then examine them, understand them and move quickly to mitigate risks. That’s why we have a team of 2500 security experts who understand how to prioritise and validate the threats that really matter.

## **Know thy enemy**

Steve Benton, BT’s Deputy CSO, and General Manager, Cyber & Physical Security Operations, talks about the importance of knowing your enemy. “We changed our stance on getting ahead of a changing landscape. Rather than looking at ourselves in terms of our inventory and what could go wrong, we look at ourselves as the bad guys would.”

We’re constantly monitoring and researching to get into the hackers heads, to understand their tools and techniques to get ahead.

Using hacking and surveillance tools, we look for where our vulnerabilities might be. Most organisations are likely to have more ‘stuff’ than is listed on your inventory, whether that’s old systems that no longer have owners, systems that are being worked on but not locked down properly or those that are incorrectly configured. Those are what hackers are looking out for.

We also deliberately give our team of ‘tame hackers’ time to be creative. To come up with new ideas of how they’d target us, and our customers. Seriously organised gangs and nation states are increasingly trying other routes into your organisation like physically getting into your sites or people based tricks such as phishing. Red teams can also be used to examine your own organisation from cyber, people and physical points of view to help identify weaknesses.

When you know your enemy, you can start to understand their motivations and business models, and therefore how you can disrupt those.

## **We look at three areas:**

1. Make it expensive

If it takes talent, time and money to attack your organisation, it’s less likely hackers will make the investment in the first place.

1. Make it dangerous

We work with law enforcement agencies to try to attribute attacks, with the ultimate aim of seeing them brought to justice.

1. Make their gains worthless as soon as possible

We’ve not only increased our defences around identity management, but we also monitor the dark web for lists of stolen details. We can then alert users and block access quickly, making the identity worthless.

## **Planning for the worst**

Les Anderson, CSO, BT says, “You can’t be scratching your head when a real incident happens worrying about what you do next.”

“We are battle-ready, but not battle-tested.” said Scott Mcelney, Head of Threat Intelligence & Consultancy, Clydesdale Bank.

That’s why we think it’s vital that we have the right processes, competence, wisdom and expertise to run faster than the attackers.

Steve Benton agrees. “We run so-called Black Swan scenarios, where we practice our response to serious incidents in real time and monitor how we respond.” Black Swan events are those that come as a surprise and have a major effect. Scenarios have to be realistic for your organisation and can be cyber based, like a major network outage or physical, like a terrorist attack on a prominent building. Running Black Swan scenarios, both with your operational teams and with your senior stakeholders, are key preparation steps to mitigating attacks. They are typically run in more mature organisations with established incident management services, but Steve thinks they add real value to organisations at all stages of their cyber security journey. “They might not be comfortable, but you’ll certainly improve off the back of it.”

After any incident, we review what went wrong, what we learnt and how we can defend our business better. We also review how well we managed the incident itself. As Steve Benton says, “You must set yourself up as a learning organisation. We learn, but we don’t blame. By blaming people, we create a culture where people won’t make decisions. It’s critical to move at the pace of an incident and get ahead of it. We need accountable people making decisions based on the information they have. Velocity of information flowing direct to decision making is fundamental.”

## **Mitigating the risk**

Faced with such a range of threats, it’s easy to start to worry about how best to protect yourself. As we talked about in [Five steps to cyber security leadership](https://www.globalservices.bt.com/en/insights/whitepapers/cyberjourney), you can focus too much on technology investment. Firewalls, anti-virus, malware detection, DDoS protection, and every other kind of technology to try to prevent a potential breach.

That’s not to say that investing in IT security isn’t important. But how do you decide what to budget for? How much should they spend? And on what?

The investments we’ve made have been in direct response to the changing threat landscape and the types of risks we see across our estate.

For example, in response to identity and application security becoming the new network ‘perimeter’ – the frontline targeted by cyber attackers, we’ve controlled who has access to what to limit the spread of attacks.

Distributed Denial of Service attacks are also on the [rise in both volume and duration](https://securityintelligence.com/news/ddos-attacks-increase-in-volume-and-duration-in-q1-2018/) as well as being used alongside other attacks to distract automated defence systems from responding to a more serious attack. So we improved our strategic defences against Denial of Service  attacks which limits the disruption from high volumes of malicious traffic and from slower, more sophisticated attacks that mimic legitimate data flow.

Steve Benton likens it to a forest fire.

“A simplified and flattened network created a forest that is easy to burn down. What we’ve done is insert fire breaks to stop the rapid spread of the attack across our network.”

We’ve used compartments to limit the lateral movement of attacks within our network, and we’re investing in making those even smaller, to each app having its own compartment. It’s then easy to understand how that compartment should operate and to spot abnormalities.

With the increasing threats against our network, we’ve deployed more scanning, monitoring and logging tools to identify intrusions and to detect strange data traffic as early as possible.

## **Sharing is caring**

Until recently, organisations would never talk about security and wouldn’t share insights into attacks, threats or incidents. That’s changing. We believe the sharing of intelligence is vital to improve our collective defence, and are in favour of creating trusted communities with which to share information.

By sharing intelligence, organisations can mitigate risks faster, meaning the success rate of the criminals’ drops.

Criminals now realise that the people, processes and technology inside many large organisations have become more difficult and less cost effective to breach. So where do they turn their attention? To the supply chain. That’s why we’ve adopted a more rigorous approach to auditing our suppliers’ security, like making sure our suppliers provide evidence that they comply with our security policies and contract terms.

## **Protecting your business the way we do ours**

It’s clear that regardless of an organisation’s size or sector, cyber attacks are a real and ever-present threat. With the right intelligence, policies and tools in place, it’s possible to not only stay safe, but to turn cyber security into a differentiator — setting your organisation apart from the competition.

But your time is limited and often divided between realising the promise of digital transformation and securing your organisation against ever changing threats.

We’ve honed our capabilities to be able to take our expertise to our customers to help them protect what matters most to them.

You want a proactive approach to security and to predict threats before they happen, with security built-in, not bolted on.