BAE SYSTEMS

The Intelligence Network

Safeguarding society
in the digital world.

Contents

Foreword

BAE Systems Applied Intelligence, Julian Cracknell P.04

Contributors

BAE Systems Applied Intelligence, James Hatch P.06
Vodafone, Andrzej Kawalec P.12
CyLon, Jonathan Luff P.16
BAE Systems Inc., Peder Jungck P.20
IDC Worldwide Security Services, Christina Richmond P.24
Independent Security and Business Consultant, David Shinberg P.26
RUSI, James Sullivan P.30
BAE Systems Applied Intelligence, Kirsten Ward P.34
Surrey University, Professor Alan Woodward P.38

Manifesto

A Manifesto for a safer digital world P.42

The Intelligence Network:

My vision

We need to talk about cyber. To meet the challenges of our highly-connected world, we have to stop giving cyber security the silent treatment.

Our instinctive response each time we're threatened is to contain it and hope that no one ever finds out. But how well is that serving us?

We live in a world where increasingly people share first, think later. It's an attitude that poses more than a few challenges. But what if a more open approach to sharing information could also help us to create a safer online environment for everyone?

In compiling this report, we have spoken to cyber security professionals in the UK and US, from across business, government and society. Over the course of many hours of conversation, it's become clear that in the face of an unprecedented threat, we cannot meet tomorrow's challenges with yesterday's thinking. It's also apparent that the cyber security community is made up of imaginative, creative people, who are passionate about helping to make the world – and not just their corner of it – a safer place.

This is why we're launching The Intelligence Network - an industry initiative powered by a community of like-minded global security professionals and industry influencers, who are committed to creating a safer society in the digital age.

Through The Intelligence Network we will deliver a Manifesto and provoke action to address some of the global issues that we believe will create more complexity and risk in the coming years.

We'll look at economic incentives and how the buying power of the largest corporates has driven fragmentation and complexity. We'll explore how large enterprises and government agencies could be disrupted by new and growing digital businesses. And we'll address the increasing software intensity of our world, which raises the importance of cyber security. We will advocate a move from passive, isolated cyber defence to institutionalised, active collaboration and learning that spans organisations, industries and countries.

> "We cannot meet tomorrow's challenges with yesterday's thinking."

I'd personally like to thank all of the people featured in this report, who contributed ideas that helped to create the first version of that Manifesto, while also acknowledging that it is a work in progress. Its completion and successful implementation will ultimately depend on the collaboration of the wider cyber community we hope to galvanise.

> "In this shifting landscape we need to see ourselves as part of a larger whole."

We live in a highly connected world that's in the midst of significant changes. In this shifting landscape we need to see ourselves as part of a larger whole and understand our collective responsibilities to one another. We need to think about how we protect the herd, rather than seek to outrun it.

This is, we hope, a step in that direction. It is an opportunity to bring together some of the greatest minds in cyber defence to help shape the world in front of us. I, for one, am extremely passionate about seeing The Intelligence Network come to life.

by Julian Cracknell

Managing Director

BAE Systems Applied Intelligence

Defending the digital world

How do we defend our future selves? It's a tough question, especially when most businesses and organisations aren't entirely clear what they will be defending, and from whom.

We are grappling with the fact that in as little as two or three years' time, the world will have changed in ways that are difficult to predict today. While we may not yet know exactly where digitalisation will take us, it's clear what's driving change in the short term. More and more economic activity is moving online and the Internet of Things, automation, instrumentation and increasing data abundance will continue that trend.

> "It's unsurprising that most businesses and organisations take an "inside-out" approach to cyber defence, focusing on themselves and the things they can control."

The challenge of an interconnected world

One of the principle virtues of digitalisation is its ability to overcome physical distance and bring people from all over the world closer together. But what does that mean for security?

Traditionally, we tend to think of security differently at a local and global level. Locally, security means protection of our family and home from the threats in our neighbourhood. From an enterprise point of view, it means protecting business operations, buildings, staff and reputation. When these things are attacked, we expect the laws of the local jurisdiction to be enforced, typically by the police.

When it comes to threats from other countries, we assume they will be dealt with by the government on our behalf. We expect governments to maintain the intelligence capabilities to understand threats to national security and the military capabilities to deter or respond to aggression from a foreign government or state-sponsored actors.

Physical space and geography is central to the way we think about threats, and where the responsibility lies for tackling them.

Security in the digital world

In the digital world, however, physical distance becomes irrelevant. If you're defending a business or organisation in a highly connected world, you need to be able to understand and deal with threats from all over the globe, by different actors with various motivations. Lines of responsibility also become blurred – in a world without boundaries, who makes the rules and enforces them?

With so much uncertainty, it's unsurprising that most businesses and organisations take an 'inside-out' approach to cyber defence, focusing on themselves and the things they can control.

However, this can leave them blind to the threats lurking beyond their immediate environment.

The criminal fraternity that we seek to protect ourselves against is highly connected – information, ideas and techniques are shared quickly and adapted to target a huge number of organisations across the globe. Unlike the businesses they target, cyber criminals care little for geographies or sectors.

by James Hatch

Director of Cyber Security

BAE Systems Applied Intelligence

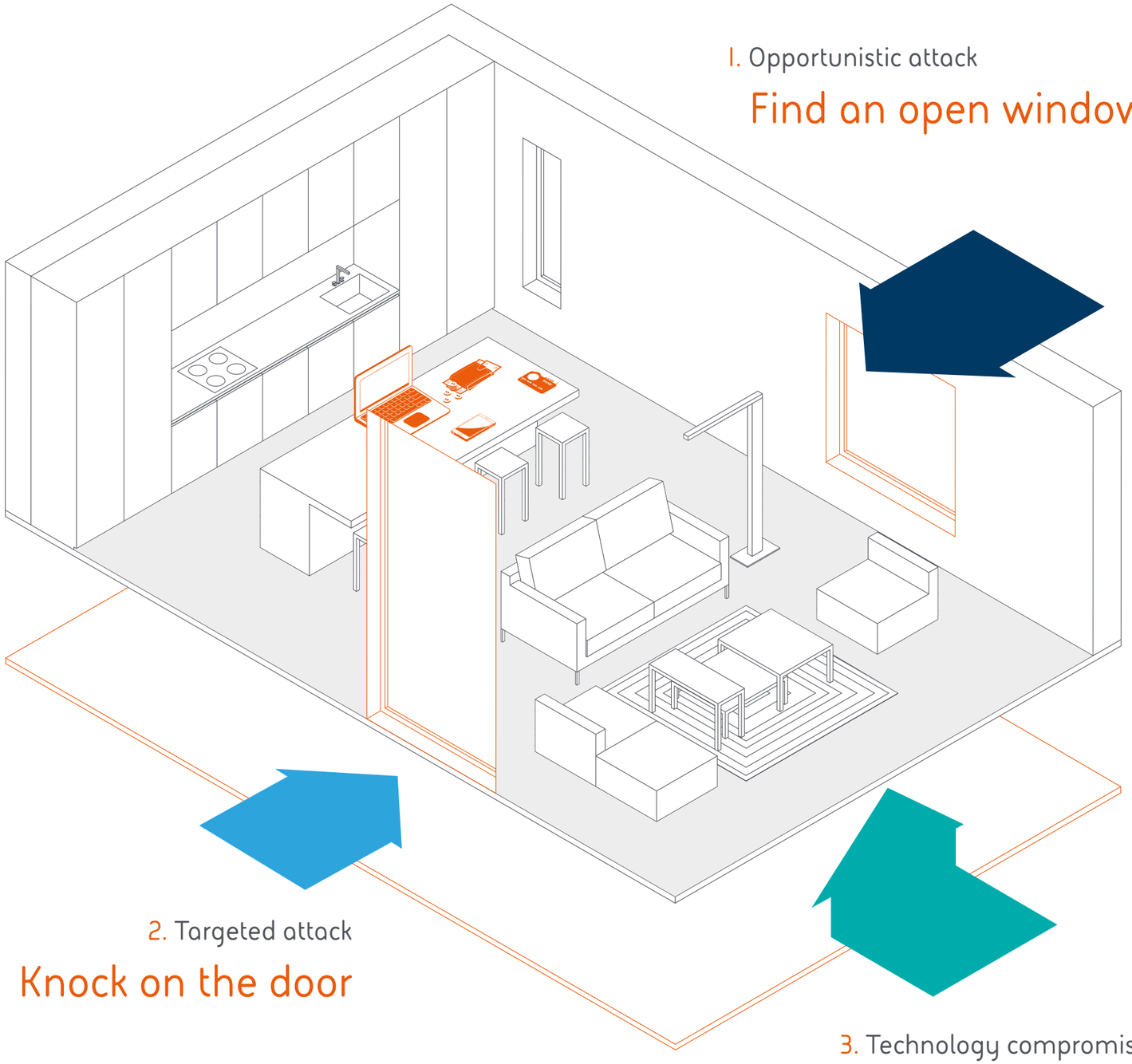
Three levels of attacks

Cyber criminals typically target us in three ways. To use a simple analogy, they start by looking for open windows through which they can enter undetected. It requires minimal effort and poses very little risk to the criminals.

If all the windows are locked, they will have to try a more sophisticated method and will knock on the front door and try to trick their way in. Organisations are increasingly subject to these types of targeted attacks and are using active monitoring and response to address them.

As we get better at defending our windows and doors, criminals are forced to undertake more difficult and costly methods. The third option available to them is to target the very foundations on which the house is built, by subverting the technology on which our business and security depends. Because of the level of sophistication required, these attacks have so far tended to be national security issues, but we should expect to see the proliferation of these techniques as we have with others.

There is a lot of inconsistency in terms of how we defend ourselves against these attacks. We still see businesses struggle to balance priorities successfully – either missing some of the basics because they are distracted by complicated security technology or lacking the capacity to defend against targeted attacks because they are too busy running around closing windows.



I. Opportunistic attack

Find an open window

2. Targeted attack

Knock on the door

3. Technology compromise

Dig through the foundations

Threat is a constant

Cyber criminals aren't going to stop trying and adapting their techniques. In the next few years the volume of threats, against which businesses and organisations will have to defend themselves, will continue to rise considerably and evolve. Ransomware attacks have increased from less than 10% of incidents to nearly half in less than two years but this balance will change again.[1]

In large part this is down to the industrialisation of cyber crime. Criminals no longer need to be adept at cyber techniques to carry out attacks. Increasingly, cyber criminals are selling their expertise to the highest bidder and turning cyber crime into a service. This new and significant criminal fraternity is lying in wait for information to become compromised. When it is, it has the capability to commit large-scale, sophisticated crime.

We've also reached a tipping point. Thanks to cloud computing, more of the information that matters most to businesses and organisations, exists outside of that organisation's four walls rather than inside it. To go back to the earlier analogy, our fixation on using technology and experts to close windows is misplaced if most of the silverware has been moved to a warehouse on the other side of town.

[1] 'Verizon 2018 Data Breach Investigations Report', April 2018
https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

Responding to a changing landscape

We are making giant leaps forward in our approach to cyber defence. Our understanding of the threat landscape, the various actors and the techniques they use to target businesses and organisations has never been greater. Venture capital and competition are driving a high level of technical innovation. And good quality guidance and information sharing forums are increasingly accessible.

But the threat landscape we face is constantly changing. It is a dynamic environment where every measure we put in place has a countermeasure. The threat to businesses, governments and society is constantly evolving as cyber criminals seek to create and exploit new vulnerabilities.

...and it's accelerating

At the same time, the number of points of vulnerability through which criminals can carry out an attack is growing considerably. The opportunities created by the Internet of Things (IoT) are massive and will significantly change the way we live and work. But without some regulation and basic security principles in place we risk being the architects of our own downfall.

The IoT is a prime example of our wider attitude to technology and digital services. In most cases, economic incentives lead developers to prioritise speed to market and customer experience. Security is, at best, a secondary consideration.

We call this a good persona bias – technologies and digital services are designed with the assumption that the person controlling their use is doing so with good intentions.

Security tends to mitigate against the potential misuse by a bad persona, but this usually happens later on in the process rather than being built into the design. The focus is on how to create the best experience for the customer, rather than the most secure.

As well as creating a larger threat surface area, we're also likely to see criminals' speed of operation outpace human security management and operations. A degree of automation already exists in which criminals use bots to find and hijack vulnerable servers. Automation presents as many opportunities to criminals as it does businesses and we should expect to see it incorporate increasing levels of intelligence. Furthermore, a security breach could spread further and faster as business and society become more automated.

> "The focus is on how to create the **best experience** for the customer, rather than **the most secure.**"

We need to **think like criminals** to respond to change

The introduction of General Data Protection Regulation (GDPR) across the European Union is changing the way society thinks about data ownership. The time is right to create a new cyber culture; one that puts creativity, collaboration and imagination first.

There are three huge changes happening right now. The first is the emergence of a more dynamic threat environment. We face adversaries who are more sophisticated and collaborative than ever, and in some instances are backed by nation states.

A lot of traditional criminal gangs and cartels are moving into cyber crime due to lower risk and higher value opportunities. This has resulted in the creation of hybrid criminal gangs – established organised crime and drug cartels working with cyber experts to circumvent security measures.

The second wave of change is the rise in regulation and greater public awareness around privacy. The introduction of GDPR in Europe this year will have far reaching consequences around the world, while the recent revelations about Cambridge Analytica and Facebook have pushed data privacy to the forefront of public consciousness.

> "A lot of traditional criminal gangs and cartels are **moving into cyber crime** due to lower risk."

GDPR is the beginning of an exciting change in how we perceive the ownership of data. Ownership is being returned to the people and companies will become merely stewards of that data. It will force enterprises to take data security seriously. I also think when people start to understand the rights available to them we'll see another big change.

Lastly, we're seeing huge technological change. New types of devices, robotics and the IoT are creating new and different ways for people to interact.

by Andrzej Kawalec
CTO, Head of Strategy
and Innovation
Vodafone Enterprise
Security Services

Where do your priorities lie?

These three elements are creating an uncertain security landscape and increasing the attack surface area. As an organisation, where do you focus your resources? The truth is you need to address all three at the same time, which for most businesses can be challenging given the talent, capability and financial resources available.

If you are a large business and you can attract and retain security talent, then great. If not, companies can increase their capability through partnerships with people who have deep security expertise.

> "You can't defend yourself against **something you can't see.**"

The cyber culture club

We need to change the culture of cyber within organisations. A company's value is in its people and you can't treat them like robots. Creativity, freedom and imagination create fantastic businesses, so we can't sacrifice those things. But every employee and partner should understand their role and responsibility in keeping the business secure.

You can't defend yourself against something you can't see. Companies should be asking themselves: How can I see the bigger picture outside of my organisation? There are companies who can help you build a greater sense of what you're defending yourself against. You don't have to do it alone.

The only way is ethics

Businesses taking a strong stance on data protection and data ethics, and enshrining that in a role, will also do well. When you look into a lot of high profile data privacy incidents, those companies could have avoided many of the problems if they had an effective Data Ethics or Data Protection Officer.

From a broader perspective, a cyber culture czar would be useful – someone who creates and enhances a culture of data awareness. If we could encourage people to become more data aware, that would have a huge impact across society.

Learning from the criminals

It's a misconception that we're behind cyber criminals and that they can attack us at will. From a tech perspective there isn't a huge gap.

To close it further, we need to mirror the behaviour of cyber criminals and get better at things like collaboration and information sharing. There are other things we can learn from them as well. For example, most companies have an annual budget cycle and three-year strategic reviews – but criminals don't behave that way. They are far more dynamic.

Create a more inclusive model for collaboration

At a national level, governments and large businesses are trying many different things across intelligence and response, and that collaboration is going well. To a certain extent, I think a lot of small businesses feel excluded from the conversation taking place. We need a collaborative model that works for businesses of all shapes and sizes, and helps to create a more complete picture of the threats we face.

We don't collaborate well at a global and grass roots level. Globally, there are huge differences between national governments and their views on data privacy. There are still very few ways to share information and collaborate across borders, particularly with law enforcement.

> "GDPR is the **beginning of an exciting change** in how we perceive the ownership of data."

by Jonathan Luff
Co-founder
CyLon

It's time to turn information sharing on its head

We need to rethink models of collaboration, with small businesses and large enterprises working hand-in-hand.

Until recently, UK public authorities had access to unique insights on cyber security. These insights could be shared with businesses and organisations to help shore up their defences against active and emerging cyber threats.

That advantage has now disappeared, primarily because of the rate of technological and commercial change. Expertise and insight within parts of the private sector now equals or surpasses that of the Government.

We need to build a system where information flows both ways and which allows us to create a broader picture of the threat landscape. I believe this is achievable, but it will require a shift in mindset and a huge amount of trust that all shared or pooled information will be used appropriately.

"It will require a shift in mindset and a huge amount of trust that all shared or pooled information will be used appropriately."

We can take the aviation industry for a best practice example. 'Black box' flight recorders are fitted inside every aircraft and facilitate the investigation of accidents and incidents. If there's a pilot error or near miss, there is an automatic assumption that no one is held responsible, as long as incident information is shared immediately. It is a well-established framework that places far more value on the sharing of information than the attribution of blame. We need to emulate that model in UK cyber security.

Keeping up with the criminals

Today, the default assumption is that cyber criminals are quicker and more advanced than those trying to counter them. In some instances, that is true, but it is far too great a generalisation.

Cyber criminals have used creativity and collaboration to operate at the cutting edge of technology. From a cyber defence perspective, we should be focusing on the same things.

Smaller businesses can move just as quickly as attackers. For larger companies, it can be more of a challenge.

At CyLon, we've built a model for collaboration that puts fast-moving innovators and their companies in direct contact with larger organisations. For small businesses it is an opportunity to test their technologies and validate product-market fit in an enterprise environment. For the big businesses, it provides access to nimble, forward-looking products and solutions.

> “We can’t simply lay **the blame** at the door of tech companies and big business.”

The impact of information sharing

In terms of collaboration between business and government, we have yet to see enough evidence that it’s working. Of course, that may be because tangible results are kept private. But in order to achieve the kind of impact seen in the aviation industry, we need to make it clear that collaboration is delivering real value to encourage more players to take part. The value of information sharing accelerates as the network grows.

At CyLon we have made an effort to build confidence in this approach, giving our enterprise partners a sense of the value that comes from becoming part of a collaborative network.

Cyber security is now having even greater impact on most aspects of organisational decision-making. Every business should elevate highly-capable employees with expertise in cyber security into strategic decision-making roles. Effective cyber information sharing at executive level will help mitigate against financial and reputational impacts that may arise from inadequate preparation.

> In terms of collaboration between business and government, **we have yet to see enough evidence** that it’s working.”

We need to take responsibility for our actions

Ethics around privacy have come into focus in the last year, but we can’t simply lay the blame at the door of tech companies and big business. We have to look at the decisions we’ve made as consumers. We have been happy to trade off utility for privacy, even if we did not appreciate the nature and scale of that trade-off.

We now need to have important discussions about the ethics of privacy in a data-driven age. It has not been debated effectively or sufficiently to date.

GDPR compliance needs to become a business advantage

The implementation of GDPR in Europe is a good start, but we should be asking, ‘what’s next?’ It is not just a case of going further, but whether data governance can become a competitive advantage for those who maintain high standards.

Good businesses won’t drown under the weight of implementing changes. Implemented well, these changes will make them better, more trusted by customers, and more desirable as places to work and do business.

That’s what regulation can and should do: set apart those who comply as outstanding partners with whom to do business. The degree to which regulatory change acts as an advantage and a stimulus for business will determine its success.

Who's on your team?

We've been asking ourselves the wrong questions about cyber defence and trying to defend ourselves in isolation. Information sharing can put you a step ahead of attackers and help you to build a cyber-resilient business.

When an attack is successful, organisations tend to put too much emphasis on questions, like: 'Who attacked?' 'How were they successful?'

While these answers are important in understanding a specific incident, and for developing a response plan and remediation tactics, they do little to prepare an organisation for the next attack. The question organisations need to spend more time focusing on is: 'Why would attackers be interested in targeting us?'

If an organisation knows why it might be a target, it can begin to develop profiles of its potential attackers. This in turn enables organisations to better anticipate potential tactics their attackers will use and the resources these attackers will have at their disposal. For example, companies that manage utilities and companies that manage finances are likely to have very different attackers, who use completely different tactics, for very different purposes. This is incredibly important information, as it enables organisations to anticipate, prepare, and enhance their defences proactively to best prepare for an attack.

No organisation is an island

There are simply no magic bullets when it comes to cyber security. No organisation has the resources to add new software, tools or analysts to address every new threat – it is just too expensive. This is why organisations that approach their cyber risks alone are acting recklessly.

While some organisations may baulk at the idea of sharing information about the types of threats that target their networks, several global industry groups and trade organisations regularly share relevant cyber threat data, and they do so securely.

This free exchange of threat intelligence enables organisations to learn about emerging threats early, providing them the window of time necessary to beef up their own defences before they themselves become a target or victim.

The crowdsourcing and sharing of cyber threat data can help us all reap the rewards of a safer cyber space at a reduced cost. BAE Systems is proud to be the leading provider of cyber threat intelligence to the US Government because we are firm believers that cyber security is a globally shared responsibility.

by Peder Jungck

President of the IT Information Sharing and Analysis Center and VP/GM of Intelligence Solutions

BAE Systems Inc.

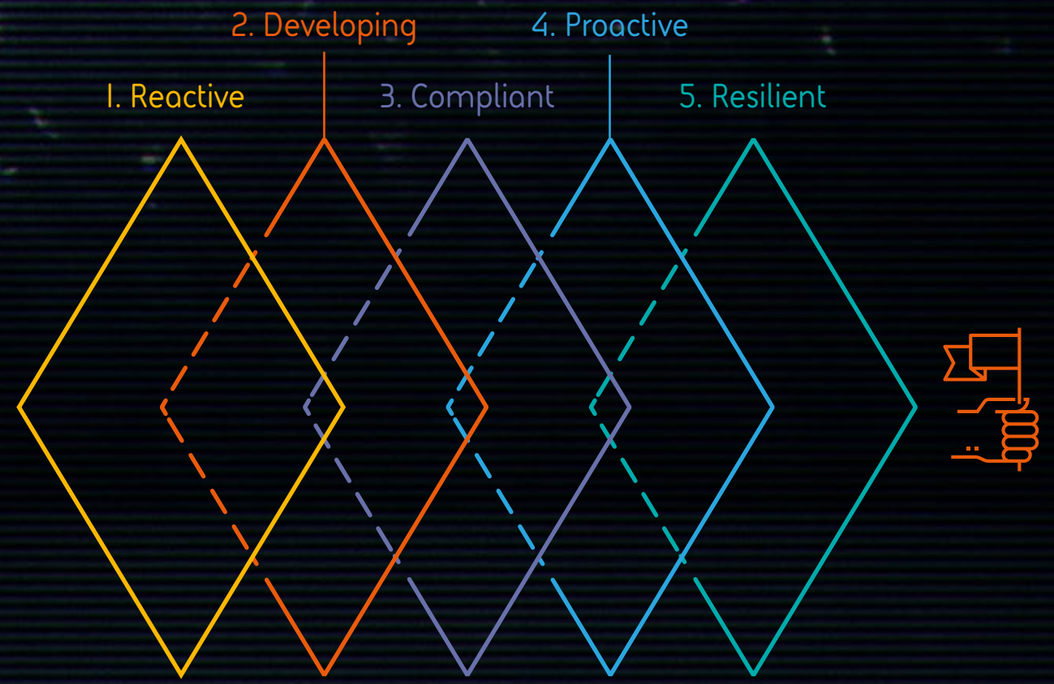
Building your cyber resilience

Businesses that manage cyber security the best are those that understand their networks and confront their vulnerabilities and actively study the objectives and trends of their potential attackers. These cyber leaders are continuously tweaking and modifying their defences to mitigate threats and reduce risk.

These 'cyber-resilient' organisations are also likely to share and exchange cyber threat intelligence with their industry partners. Companies that are well-informed about their own networks, risks, and adversary trends are most likely to have effective automated defence solutions that help their experts monitor, flag, and isolate common attack signatures to stop threats in their tracks. This frees up resources and allows their network experts to focus their attention on suspicious activities and network anomalies which could otherwise be overlooked.

> "Businesses that manage cyber security the best are those that understand their networks and confront their vulnerabilities."

To rank the effectiveness of an organisation's cyber defences, companies should assess their progress and performance using a five-tier Cyber Security Maturity Model. There are multiple variations on these maturity models, but in general, companies rank their defences as follows:



The tiers described on page 21 determine how proactive, innovative and mature your organisation is in continuously evolving to stay ahead of the threat. A Reactive organisation is one that implements policies, training and tools as a result of a breach, regulated assessment or major market initiative. Organisations in the Developing group typically feature established basic processes, identified a Chief Information Security Officer (CISO) or key team with organisational support to improve security posture. A Compliant organisation is one that regularly measures the state of cyber, trains its employees and establishes a roadmap to keep up with the known threats.

A Proactive organisation is one with established means to reach out, involved in community collaboration and proactively works to stress the organisation leveraging cyber security posture for competitive advantage. A Resilient organisations understand the impact of cyber risk, has a means to operate during the worst of events and continuously prepares for scenarios while driving market leadership in contingency planning.

> "A resilient organisation is one that **understands the impact of cyber risk,** has a means to operate during the worst of events and continuously prepares for scenarios."

It's a game of cat and mouse

Network breaches are like cancer. The longer attackers hide within the body of the network, the more damage they can cause. It is imperative that organisations reduce the dwell time of cyber attackers. To accomplish this, organisations must be constantly updating their security standards and patching vulnerabilities. They must also invest in automated solutions that can help detect suspicious activities and alert analysts when these anomalies are identified.

It's really a cat and mouse game where stealth wins. Far too often, businesses try to react to attacks and patch issues or remediate their networks once the damage is done. If their posture does not change, and they fail to take more proactive measures in the future, they are likely to be targeted again.

This is because most attackers gravitate to easier targets where it's easiest to succeed and remain undetected. Meanwhile, organisations that are the most vigilant in updating their security protocols are most likely to frustrate and annoy attackers into choosing other softer targets. Remember, it takes months for cyber attackers to choose targets, conduct research, develop software or malware to carry out attacks, perform tests, and then launch strikes. If, by the time the attacker is ready to attack, the target has already anticipated and blocked the attempt, the attacker is likely to choose another target rather than start over.

The same logic holds true if, after months of preparation, security experts are able to quickly flag a breach and minimise the threat before it can cause impact or harm.

This is one of the primary reasons 'dwell-time' is a statistic most business boards of directors use as the benchmark when assessing the security and performance of its network. It's the best statistic to assess how effective its security measures are at mitigating cyber risk.

> "Organisations must be **constantly updating their security standards** and patching vulnerabilities."

The impact of information sharing

Most cyber threats have sensitive indicators and warnings, including malware signatures, malicious IP addresses and common attack tactics and techniques. Do you know why? It's because our adversaries are excellent at sharing information on how to break into corporate networks.

Organisations can reduce their risk and improve their cyber posture by following suit and regularly sharing timely threat indicators and effective defensive measures. Sharing this information enables all members to quickly enhance their defences and implement more informed risk management strategies.

Sharing the combined cyber threat knowledge of multiple companies can make a huge impact on a business' cyber ecosystem by minimising threats across an industry and enhancing the effectiveness of each organisation's defences without requiring additional resources. Cyber threat intelligence sharing is a critical cyber defence force-multiplier in which more organisations should consider participating.

Going beyond compliance

Regulation is changing the way we think about data privacy, but it's also creating security blind spots. We need to stop thinking of cyber security as a tickbox exercise.

Businesses take regulation seriously and put a lot of resources into compliance. It's good the basics are taken care of but it can make businesses blinkered and create the misconception that if you're compliant, you're secure. You need to see the bigger picture.

GDPR is changing the way we think about data privacy in Europe and it's likely we'll see a GDPR equivalent in the US and other countries around the world. I imagine those conversations are already starting. It's setting a new standard for multinational companies and it's likely that those same companies will expect every business in their ecosystem to work to that same standard, irrespective of where they are located.

Beyond compliance, businesses should be taking a much more proactive approach to security and have a strategy to work to. The time you invest in it will be paid back and it will stop you from being solely reactive.

Enterprises tend to be better at thinking long term. They also know where the gaps in their knowledge are, whereas a lot of smaller businesses don't know what they don't know.

In that situation, cyber threat intelligence sharing between businesses becomes vital. But I think it's overwhelming for (SMEs). Suddenly, they have access to all this data and they don't know what to do with it. We have to find a way to put actionable data in the hands of SMEs.

Simplifying and gamifying security

Simplicity is key. I'd like to see good security practices made easier and where possible, enjoyable. We're all coin-operated, so businesses should be rewarding employees and incentivising the right behaviours. If we could gamify good practice, we could change the mindset around security so it becomes less of a burden and more of an opportunity. Employees could earn points that could be exchanged for time-off or financial benefits.

We need to make security fun. I'd also like to see security become an emblem for better brand performance. Rather than using fear, uncertainty and doubt, it should be a conversation about strengthening the brand. Security becomes a score, similar to a credit rating, so everyone can understand the level of security they can expect interacting with that business.

Christina Richmond
Program VP
IDC Worldwide Security Services

AI is changing how we detect and respond to attacks

The rise of machine learning and AI is helping us to combine huge volumes of geopolitical system-based information and human-based information and turn it into something that we can ask questions of.

It's not going to be a panacea. But it's a huge assist in terms of accelerating how we detect and respond to attacks.

It will also help with the talent shortage. If we can use machine learning and AI to help us do most of the analysis then it frees up cyber professionals to ask questions and make decisions on remediation. 'Eyes-on-glass' will still be necessary for threat-hunting and response, but AI can free people up to spend more time on critical thinking.

> "Security becomes a score, similar to a credit rating, **so everyone can understand** the level of security they can expect interacting with that business."

Protecting our digital identities

The biggest challenge we face is the complexity of our environment and our obsession with the shiny new thing and the belief that each new piece of technology will save us. As we augment ourselves digitally, we are increasingly creating versions of our identities that could be accessed and manipulated by others. It's worrying that someone could access every aspect of my life and effectively become me. We're creating huge vulnerability and risk for ourselves.

That's not going to change. I like convenience and that's what it boils down to: am I going to sacrifice convenience for the sake of security? I love the fact that an Uber driver can find me wherever I'm standing, or that my car can rescue me when I've had an accident. Unless we feel threatened, I think human psychology dictates that we'll always opt for convenience over our concerns for the risk.

> "If we could gamify good practice, we could change the mindset around security so it becomes **less of a burden and more of an opportunity.**"

Secure by design

Once it was central to the design process, but security has slipped down the pecking order. As the volume of cyber attacks increases, we need to return to less haste, more security.

> "Most people will spend money looking for the one-in-a-million attack rather than making sure they can constantly repel daily attacks."

Around Thanksgiving last year, I found out my credit card was compromised and used in South America. My bank contacted me, letting me know that there had been fraudulent activity, and sent me a new credit card.

I was really careful with my new card and only used it in three places before it was compromised again. I spoke to my bank and after a period of time discovered there was a crime organisation that was auto-generating credit card numbers and trying millions of them until they worked. Once they found a card that worked, if the bank wasn't fast enough to detect and block it, they cashed in.

It seems incredible that I was the victim on two occasions within a very short space of time. But when you think about credit cards, the first eight digits are easy to guess. With the technology available today, it isn't difficult to quickly randomly generate and test millions of credit card numbers.

Understanding the risk

The threat to small businesses is much greater. Most people will privately admit they pay less attention to their business credit card statements than they do their personal ones. Unless you have rigorous accounting processes in place, attacks like the one I experienced may go unnoticed for longer, especially if your workforce does business across lots of different countries.

Small and medium businesses often fail to understand the true risk they face. Any cyber security professional can make a company more secure – they just have to ask every employee to switch off their Internet connection. However, it will quickly become non-profitable and close within a matter of weeks. Security is about understanding and accepting a certain level of risk.

Most people will spend money looking for the one-in-a-million attack rather than making sure they can constantly repel daily attacks. A lot can be achieved simply through employee awareness. Do they know not to respond to phishing emails? Do they know not to open malicious attachments? Are they blocking USB devices?

Cyber criminals will always look for the easiest way in. If I were an attacker and wanted to target a company it costs me nothing to send an email to thousands of employees and there's very little risk to me.

If that's unsuccessful, it's much harder for me to go and sit in that company's lobby and try to hack into their WiFi, so I won't do that. Instead, I'll move on to the next company and send them thousands of emails, and then the next company, and the next, until I'm successful.

> "When I started out in computing, security wasn't a separate consideration, security was just how you designed good systems."

David Shinberg

Independent Security and Business Consultant

Security is coming second to speed

When I started out in computing, security wasn't a separate consideration, security was just how you designed good systems.

Thirty years ago, when I was in college, a friend and I wrote a programme of about 1,500 lines and we got an A. Another friend wrote a programme and also got an A, but hers was 1,000 lines. We did a lot more work than we had to because we thought that was the right way to write a programme, to check for everything.

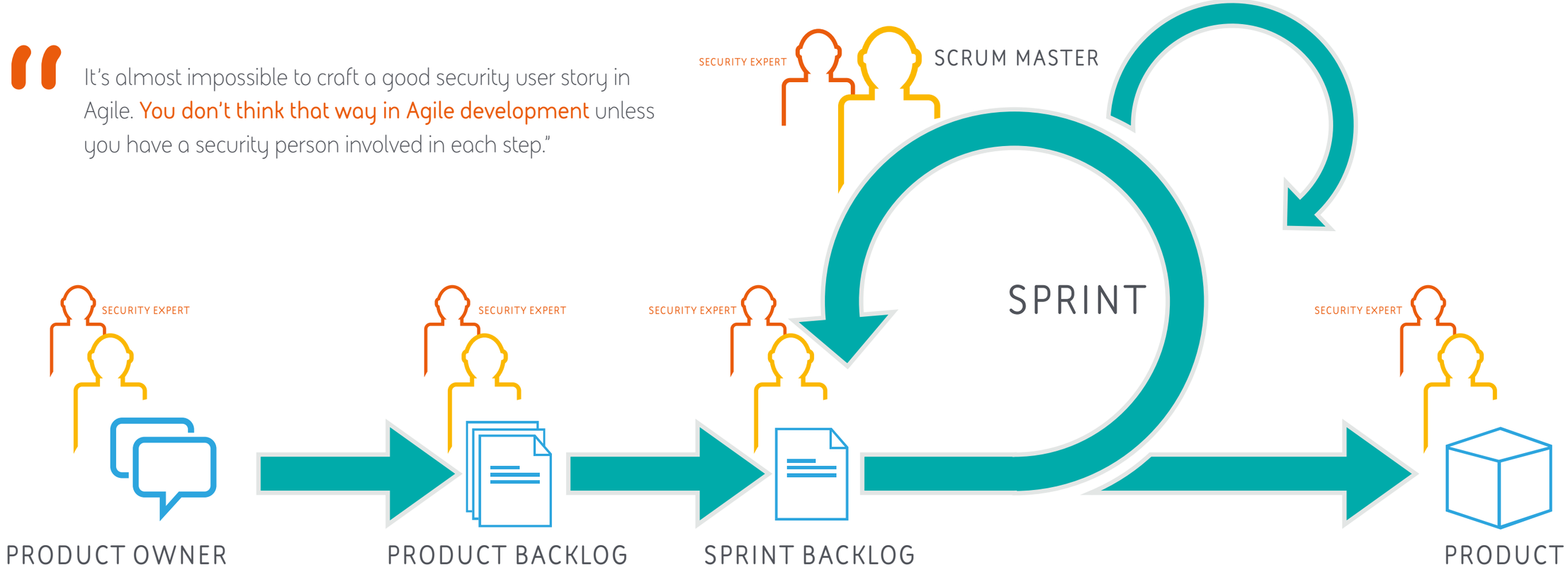
For a number of years, that's been totally lost on people, especially in smaller, faster moving businesses where the aim has shifted to making things work as quickly as possible.

Security stopped being a consideration during the design phase. Take the Agile methodology for example. It's almost impossible to craft a good security user story in Agile. You don't think that way in Agile development unless you have a security person involved in each step.

> "Most businesses today are secure to the point that they're compliant and, **unfortunately, I think that will continue** to be the focus."

Most businesses today are secure to the point that they're compliant and, unfortunately, I think that will continue to be the focus, particularly with the introduction of GDPR. In the case of GDPR, my concern is that for businesses outside of Europe, if they don't have enough exposure, there's a risk they'll stop doing business in Europe completely. In many ways, I think it goes too far in protecting individuals. I would never consider a business address, email or phone number to be personal information. I'd consider it a company asset.

> "It's almost impossible to craft a good security user story in Agile. **You don't think that way in Agile development** unless you have a security person involved in each step."



Shaping tomorrow's cyber strategy

Individuals tech giants and government: we all have a role to play in creating a cyber security culture that can stand up to the unprecedented threats we face.

In April this year, the National Cyber Security Centre (NCSC), Department for Homeland Security (DHS) and Federal Bureau of Investigation (FBI) issued a technical alert warning of malicious cyber activity attributed to the Russian Government. Threat actors are targeting government, private sector, critical infrastructure and Internet service providers (ISPs) supporting these sectors.

The UK has a mature national strategy that communicates strategic information about cyber related threats and challenges. It is a strategy that compares favourably to those of other nations.

To keep pace with the evolving threat landscape, the next iteration of the UK's cyber strategy should further set out roles and responsibilities of the different sections of society in reducing the cyber threat. We should be asking ourselves these questions and addressing them now. Cyber security is not the sole preserve of government.

Creating a security culture

We are trying to reduce cyber crime because it has a negative economic and political impact for all of us. It is a national issue so we should all feel a sense of collective responsibility. At the moment, there is a risk that although organisations are concentrated on securing their own networks and data, there is not much thought given to the wider sociopolitical and economic challenges we face from cyber threats.

To start with we can do better at education and awareness. We need to show people that they have a responsibility and an active role to play in improving cyber security, rather than expecting others to protect their data.

We should also be encouraging people to train in subjects that lend themselves to careers in cyber security. We need to show people what a career in cyber looks like and reward them accordingly for pursuing one.

A job in cyber security has real purpose and is as much about understanding people as it is about technology. Not everyone has to be technologically-minded. For example, there is a role for those who can process complex information and help simplify the sometimes overly technical language that is associated with cyber security.

by James Sullivan

Cyber Programme Lead

Royal United Services Institute for Defence and Security Studies

I would also like to see a lead on online culture and behaviour; someone who can educate people about the information we put online and how we use the Internet and social media. It is alarming to think how much personal information we share online and how quickly that has happened.

The revelations about Cambridge Analytica and Facebook should serve as a wake-up call for Internet users. Did we really think when companies were collecting information about us that it would not be exploited somewhere along the line? It was inevitable.

> "It is alarming to think how much personal information we share online and **how quickly that has happened.**"

With great power comes great responsibility

Technology companies and digital service providers themselves have a responsibility to educate their users about how their personal data will be used, the risks involved, and what they are doing to mitigate threats. That has not always happened, but I think it is starting.

Facebook recently removed content by Russia-based disinformation actors and has published further steps it will take to protect user privacy.

Helping people to understand the threat is key. That has traditionally been the role of the Government, but increasingly tech companies are expected to provide threat and impact assessments.

> "We need to show people that they **have a responsibility** and an active role to play in improving cyber security."

The role of legislation

In terms of regulation and legislation, we have had a 'carrot' approach up until now. The UK is moving more towards the 'stick' approach through GDPR and the Networks and Information Systems (NIS) Directive. An appropriate balance between hard and soft power will be difficult to achieve. Technology will always move faster than legislation and regulation alone is unlikely to deter attackers.

It is still early in terms of the role of legislation and it would be regrettable if this were deemed to be the main solution in reducing cyber crime. We should look at ways to encourage people to share cyber threat intelligence more, rather than force them to do so. The best way to do that is by demonstrating the positive impact of sharing information over time and publicising those benefits. It is about building trust across society.

Understanding the threat we face

We have a good understanding of the threat landscape, but there are a number of challenges we are yet to overcome. There is a lot of cyber threat intelligence available, especially when you think about it at an international level. How do we coherently aggregate all that information and draw strategic conclusions from it? How do we improve cyber crime reporting? It is not happening at all at the moment, but GDPR may change this.

The NCSC does a good job of helping people, businesses and organisations to understand the risk. But looking beyond the NCSC, I think there should be a shift to providing clearer and simpler information to people.

> "Did we really think when companies were collecting all this information about us that it wouldn't be exploited somewhere along the line? It was inevitable."

It starts with intelligence

Combating the unprecedented threat we face is contingent on recognising the similarities between cyber criminals and cyber professionals, and thinking differently about the roles of both.

Over the past few years we've seen a lot of change and we expect that to continue being the case. In the last year we've seen a big increase in the number of supply chain attacks – such as NotPetya and CCleaner. We expect threat actors to continue targeting the supply chain as an effective way to exploit the vulnerabilities, rather than attacking the victims directly themselves.

We've also seen geopolitical issues correlating with behaviours in cyber space. We're likely to see that intensify as nation states respond to events happening in the real-world. There's been a lot of cross-over between nation state and criminal actors which has emboldened many individuals. A growing number of cyber criminals now have nation state capabilities at their disposal and are also less worried about attribution.

Artificial Intelligence in the kill chain

AI is very interesting. There are lots of different definitions around AI – I would describe it as a machine that can complete tasks that are characteristic of human intelligence. Using that definition, it's clear it's already commonly used in cyber defence, specifically in things like fraud, threat and anomaly detection.

So far, AI use by threat actors has been limited to disinformation campaigns on social media. In the future we could see attacks that attempt to confuse AI through malware, fraudulent activity, or deliberately distracting it through increased network traffic. I don't think it's likely we'll see an end-to-end attack using AI any time soon. Threat actors still need human intelligence in the kill chain.

> "A growing number of cyber criminals now have **nation state capabilities** at their disposal."

Kirsten Ward
Cyber Researcher
BAE Systems Applied Intelligence

An intelligence-led approach

On the other side of the fight, organisations are beginning to realise it's important to be secure by design and that it is much harder, and less effective, to add security in at the end.

Businesses need an intelligence-led assessment of their entire organisation. Then they must apply an understanding of the cyber threat landscape to the organisation's people, processes and technology to reveal the risks they face and how an attacker could exploit them. This helps them to become more proactive in the way they protect themselves.

> "There's a **misconception** that you need to come from a technical background to pursue a career in cyber defence."

Rethinking cyber roles

More progressive organisations also recognise that security teams need a range of people that bring different backgrounds, skills and opinions to the table. There's a misconception that you need to come from a technical background to pursue a career in cyber defence.

A member of my team has a geopolitical background – she studied War Studies at university. She's helped to develop our understanding of geopolitical events that have implications in the cyber world.

Businesses should look in the less obvious parts of their organisations for those hidden gems and should recruit for the right mindset rather than simply the right technical profile. For example, how do candidates approach logical thinking? Can they work across open sources of intelligence and analyse complex information? These types of people are far more likely to have studied English or History than more traditional STEM subjects.

Finding common ground

Cyber criminals share a lot of similarities with cyber security professionals. One threat actor we track is highly capable and incredibly professional in terms of how it's structured. From the outside it appears to be just a normal tech company, with developers, project managers, and even an HR team. Similar to any other business, that corporate structure improves its overall capability and effectiveness.

However, those organisations have fewer barriers. They don't have to adhere to the rules and regulations that most businesses do, which makes them a lot quicker. I should note, it's wrong to characterise all threat actors as immoral, not least because it limits how we respond to them.

Last year, we became aware of an incident where an individual's device was targeted using ransomware. The victim contacted the police who opened a dialogue with the criminals. As the police got to know the criminals, they discovered they didn't target just anyone. For example, they wouldn't target people working in schools and hospitals, or anyone within their own country. The police explained the victim's personal situation and managed to convince them to return their data.

It's not always going to be successful but we've seen that it is possible to appeal to cyber criminals' better nature. Education is also really important, especially if you can reach people at a young enough age and show them the real-life impact of things that happen online. At a societal level that's something we need to get better at for reasons that stretch beyond cyber security.

Blocking out the noise

The volume of cyber attacks is being turned up to 11. But we can't simply shove our fingers in our ears; we need to promote openness and share information about the challenges we face.

Professor Alan Woodward
Surrey Centre for Cyber Security
Surrey University

There has been a rise in the number of ransomware and malware attacks, largely due to the emergence of cyber crime as a service. You no longer have to be adept at cyber crime to carry out an attack; you can simply pay someone else to do it for you.

Rather than focusing on individuals, criminals will increasingly target data hubs – places where they can scoop up lots of information and get away with it quickly. To use a simple analogy, rather than burgling your house, they will be going after bank vaults.

Increasingly, criminal gangs are grooming younger people, particularly students, and making them complicit in criminal activities. This usually happens in one of two ways: by using their personal bank accounts; or by challenging individuals to carry out cyber attacks without being fully aware of what their skills are being used for.

People problems

To improve how we defend ourselves, we need to get better at understanding human behaviour. People will always try to find the quickest, easiest way to do things. If security gets in the way then we will find a way to circumvent it. Cyber defence is about people, process and technology and how those three things interrelate.

Awareness has to be a constant because people lose interest and become complacent, and complacency is dangerous. Cyber criminals are willing to play the long game and will wait until our collective guard is down.

We need to instil in people the idea that you should not blindly trust those you meet online. For example, we're guilty of putting our faith in security measures like the padlock symbol that appears in your browser and denotes that communications are encrypted using SSL. The communication is secure, but you still can't be 100% sure who you are having a conversation with and if they are who they say they are.

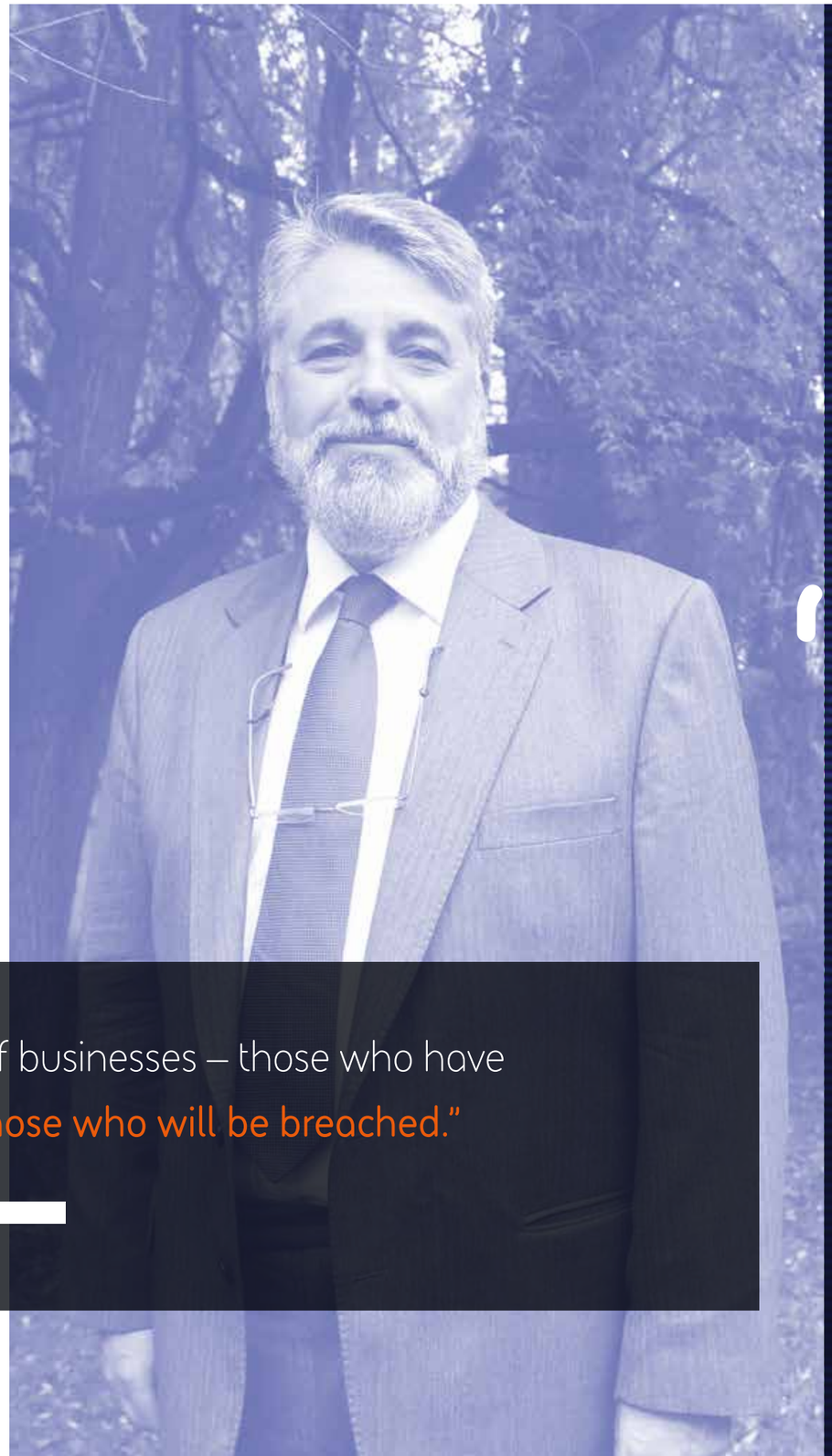
> "When you look at companies like Google, Facebook and Twitter, the argument that 'we are just a dumb pipe' doesn't hold anymore."

Kingdom of trust

As individuals, we can take all the precautions in the world, but if the businesses we trust with our data aren't equally as careful, then we're in trouble. Most people today have set up lots of personal accounts with digital service providers that contain their personal information. We should all be asking ourselves who we truly trust with our data.

When it comes to personal data stored by large businesses, there's the illusion of safety in numbers. If a company holds the details of millions of customers, what's the likelihood that my data will end up in the wrong hands?

But if criminals get access to our personal data we can be certain that it will be used. As soon as our personal data appears on the dark web, it's in the criminal supply chain and eventually, someone, somewhere will use it.



> "There are two types of businesses – those who have been breached and those who will be breached."

Putting security before growth

In some cases, large companies have failed in their moral obligation to protect users. A lot of large technology companies have grown so quickly, they haven't understood their level of responsibility in the situation they've found themselves in. They have prioritised growth over security.

When we look at companies like Google, Facebook and Twitter, the argument that 'we are just a dumb pipe' doesn't hold weight anymore. We need to work out how we define these companies and their responsibilities.

Looking ahead to the IoT, we need some regulation and basic security principles in place, similar to the Kitemark system to show consumers that devices follow certain security principles. That would help to mitigate a lot of the security risks and give reassurance to consumers. I also think there's a role for regulation in ensuring that retailers are just as responsible as manufacturers for the connected devices they sell.

> "The more information we have about security breaches, the better our understanding of the threat landscape."

A problem shared is a problem halved

When it comes to businesses there are two types – those who have been breached and those who will be breached. Businesses need to understand that we're all in it together and that we will all be affected at one time or another.

Businesses are realising that if you share intelligence in the right way, you can do it securely and without giving away any sensitive information.

The NCSC (National Cyber Security Centre) is doing a very good job of giving advice and promoting openness. Through the Cyber Security Information Sharing Partnership (CiSP) it has done a lot to promote cyber threat intelligence sharing which is already having a really positive impact.

I hope more businesses can be encouraged to share information and be transparent about the challenges they face, and their successes. The more information we have about security breaches, the better our understanding of the threat landscape. The better our understanding, the more we can do to prevent breaches happening in the first place.

I also think that we could improve attribution and publish information about who is behind a lot of the criminal activity we see. We need someone to take the fight to the criminals, make them aware they will be caught, named and shamed.

The Intelligence Network 2025:

A Manifesto for a safer digital world.

It's clear that a collective approach to changing leadership, culture, behaviour and processes is vital in tackling the evolving threat posed by cyber crime to all sections of society.

Through this Manifesto, we are setting out the ambitions of The Intelligence Network and establishing a framework for creating a safer digital society over the next seven years. This Manifesto has been created by the community, for the community, and draws on the intelligence of the industry experts featured in this report. The Manifesto is focused on three distinct areas of transformation:

We hope that it acts as a starting point for conversations about the future of cyber defence. For over four decades, we have helped to defend societies, governments and nations from cyber attacks and financial crime. Through the ambitions set out in this Manifesto and the work of The Intelligence Network, we want to invite the cyber community to be a part of the change that it wants to see within the industry. We hope to create greater transparency by inviting people from diverse backgrounds, to work as a community to solve the challenges we face in a spirit of openness, collaboration and trust.

Critical issues to address to create a safer digital world between now and 2025

The contributions of the industry experts in this report highlight a set of critical issues. Distilling these and projecting them forward over our timescale reveals three broad themes:

1. Economic incentives and the buying power of the largest corporates have driven fragmentation and complexity into the cyber security marketplace and technology landscape, at the same time as a higher proportion of organisations have recognised the need for effective cyber security. Small- and medium-sized businesses in particular don't receive the right level of support and are struggling with integration and implementation.

2. Society and its large enterprises and government agencies will continue to be disrupted by both new or growing digital businesses, and by the fast pace of development and economic growth. Existing technology, infrastructure and approaches to cyber security will rapidly become irrelevant legacies.

3. The increasing software intensity of our world and the growing use of artificial intelligence raises the importance of, and risks to, cyber security. Thriving in the face of these risks needs both technology-based innovation and an evolving model of security that moves from passive, isolated cyber defence to institutionalised, active collaboration and organisational learning that spans organisations, industries and countries.

PILLAR ONE

Collaboration

Mindset change:

Building a new culture through radical trust

Action:

We need to move from each organisation defending only themselves to organisations working together to defend everyone.

The traditional structures through which we think about businesses are becoming increasingly irrelevant in the digital age, particularly when it comes to cyber defence. Furthermore, in our increasingly connected world, if a business or organisation is breached, it poses a risk to every connected organisation, including rival businesses.

In this context, we can't defend the herd by seeking to outrun it. We need to create a collective cyber immune system that everyone contributes to and that works to the benefit of all. For this to become a reality, we must build radical trust among businesses that until now have viewed each other in adversarial terms. We must also encourage large enterprises to share resources, knowledge and expertise with smaller companies to help create a unified response to cyber crime for the benefit of all.

Informational siloes create opportunities for criminals. We need to develop not only intelligence sharing but also a collective sense of responsibility that transcends business divisions and international boundaries.

> "In this context, we can't defend the herd by **seeking to outrun it.**"

GOALS FOR 2025:

- By 2025, society can respond as one to threats at digital speed. It will do this by sharing threat intelligence, understanding, approaches, technology and resources in a co-ordinated manner.
- Aggregated, verified information is provided to the appropriate law enforcement and Government organisations and these are set up to deal with the threat through prosecution or disruption, depending on the source.

PILLAR TWO

Simplicity

Mindset change:

Don't blame the people, change the game

Action:

We intend to change the mentality around security by refocusing people on making things easier rather than assigning blame.

The prevailing approach is to forewarn people of the dangers they face and try to prevent them from engaging in risky behaviour online. We should be encouraging the behaviours we want to see through incentives and gamification, but it should also be simpler for people to do the right thing. What if rather than stopping people from clicking on links, we made good cyber practice as enjoyable and simple as flicking through their social media feeds? To truly engage people, we should create security processes that complement human behaviour, instead of seeking to change it.

It's time to stop victim-shaming businesses, organisations and people who are hacked. In the words of Professor Alan Woodward, there are two types of business: "those who have been breached and those who will be breached". A lot of businesses and organisations have been hacked despite doing all the right things. If all we do in the wake of a security breach is look to assign blame, then we discourage transparency and miss the opportunity to learn from the experience.

That is why we are seeking like-minded organisations and individuals to come together to share their experiences, to learn and to improve security for the better of society.

> "It's time to **stop victim-shaming** businesses, organisations and people."

GOALS FOR 2025:

- Security is transparent so that organisations and individuals can see what security they do and do not have in place, as well as where there are gaps and their implications.
- Technology is secure by default – both on purchase and through its life – maintaining security through automatic updates without overloading the memory and workload of individuals.

PILLAR THREE

Certainty

Mindset change:

Turn volatility into business as normal

Action:

We live in a volatile world. We need a cyber security process that turns that volatility into business as normal.

Cyber security is adrenaline-fuelled, because in a lot of cases it fails to stop the attack. This is evident because businesses and organisations still regularly suffer security breaches despite investing in the latest technology. When they do, heroes in the form of cyber security experts fly in to save the day. Often these efforts are only a temporary sticking plaster that covers the wound, but doesn't cure the problem.

We need to focus less on heroes and technology, and increasingly on the more reliable world of competence and procedure. We may have to move beyond the era of cyber security being exciting and unpredictable, and create a world where we can respond to uncertainty and constantly changing threats in a reliable, measured way without disrupting 'business as usual'. Volatility, fear and uncertainty do not help us to address the problem.

Cyber security should not be an opaque world that is understood by specialists, but shuts out everyone else. We need to create transparency and a degree of readiness, so people are no longer surprised by security breaches and are well prepared to act decisively when they find themselves under threat.

> "We need to **create transparency** and a degree of readiness."

GOALS FOR 2025:

- Cyber security is a mature enough discipline that organisations and people within them understand what they need to do in different situations and are able to do this efficiently and reliably. Security is available as an affordable utility for those that need it.
- Boards can have confidence in the security measures in place within their businesses and cyber security can be managed through standard corporate risk management structures in the same way as health & safety or financial risks.

Early recommendations for steering group **discussion**

The Intelligence Network Steering Group will build on the founding ambitions of the Manifesto for change and explore ideas, initiatives and programmes that help to achieve its aims.

Based on the findings of this report, in the short term the steering group will explore the following questions:

- **How can we help** businesses and organisations rethink the boundaries for security and build a model for global collaboration?
- **Is it possible to create** a collaborative model for private and public sector that ensures a mutual level of responsibility and investment?
- **How can we foster** a culture of simplicity and transparency in cyber security and make it accessible to a greater number of people?
- **How do we create** an environment within businesses and organisations to improve the confidence and understanding of the business risk and handling of cyber attacks?

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

E: theintelligencenetwork@baesystems.com | W: baesystems.com/theintelligencenetwork

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai