McKinsey&Company

Defense of the cyberrealm: How organizations can thwart cyberattacks

January 2019

Governments and companies have much work to do to protect people, institutions, and even entire cities and countries from potentially devastating large-scale cyberattacks.

In this episode of the *McKinsey Podcast*, Simon London speaks with McKinsey senior partner David Chinn and cybersecurity expert Robert Hannigan, formerly the head of GCHQ,[1] about how to address the major gaps and vulnerabilities in the global cybersecurity landscape.

Podcast transcript

Simon London: Hello, and welcome to this edition of the *McKinsey Podcast*, with me, Simon London. 2018 was a year of good news and bad news in cybersecurity. The year passed without a major international incident, certainly nothing on the scale of the WannaCry ransomware attack, in 2017. And yet every few weeks brought news of another big data breach at another big company. So where do we stand going into 2019? Are we winning, in any sense? When and where will the next so-called tier-one attack occur? And, importantly, what is the role of government in helping to ensure national cybersecurity. To find out more, I sat down in London with David Chinn, a McKinsey senior partner who works with public- and private-sector organizations on these issues, and also with Robert Hannigan, who is the former head of GCHQ, the UK government's electronic-surveillance agency. Robert also led the creation of the UK National Cyber Security Centre, or NCSC. Today he's a McKinsey senior adviser. Robert and David, welcome to the podcast.

David Chinn: Thank you, Simon. Glad to be here.

Robert Hannigan: Thanks.

Simon London: I think for a layperson, the general question around cybersecurity is, probably, are we winning?

Robert Hannigan: No, I think we are making progress, but I think it would be very rash to say we're winning. If you look at the two big trends, the rise in volume of attacks and the rise in

[1] *Government Communications Headquarters.*

sophistication, they are both alarming. On volume, particularly of crime, there were something like 317 million new pieces of malicious code, or malware, [in 2016]. That's nearly a million a day, so that's pretty alarming.

On the sophistication, we've seen, particularly, states behaving in an aggressive way and using very sophisticated state capabilities and that bleeding into sophisticated criminal groups. It's a rise in the sheer tradecraft of attacks. So no, I don't think we're winning, but I think we're doing the right things to win in the future.

David Chinn: I would agree with Robert. We may not have seen a single attack that brought down multiple institutions in the same way that WannaCry did, but look at the list of institutions reporting very sizable breaches of increasingly sensitive data.

Now we've got some more regulation forcing people to be more transparent about the breaches and the length of time that attackers were inside networks before being discovered. And it's not always clear to those attacked what they've lost. I'm broadly pessimistic.

Simon London: When you think about where the next tier-one attack might come, what are some of the vulnerabilities that in business and government people are thinking about, talking about?

Robert Hannigan: I think most of the focus now is on supply-chain and upstream risk, because even the best-defended companies now realize that their vulnerability is either those who are connected to their vendors, their suppliers, even their customers. And, increasingly, government is worrying about the IT infrastructure, so the global supply chain, both hardware and software, and its integrity.

And some of the state attacks we've seen in the last couple of years have been against the backbone of the internet, if you like. Routers, switches, places that give you massive options to do different things with internet traffic [Exhibit 1]. It's going deeper and more sophisticated.

David Chinn: I think there's different versions of what tier one might feel like. I think that the increasing ability of both criminals and states to attack critical infrastructure [is one of them]. Taking out power to a city might have relatively limited impact in terms of the actual damage done, but could have a huge impact on the way people feel.

Robert Hannigan: There's a difference between a genuinely catastrophic damaging attack and a politically sensitive attack that spreads fear and terror or a lack of trust in data. It's fairly easy to imagine things that will lead to public panic.

You've seen big public controversies over airlines and banks being unable to function, often not through cyberattacks. But if you were to multiply that and see it as a malicious attack, you could see genuine public disquiet, a lot of political pressure to do something about it.

Simon London: Yes, it's interesting, because when you talk about critical infrastructure of the modern economy, you often think about things, like, as you say, the internet backbone.

Exhibit 1

Companies should assess threats and develop controls to the most critical.

Assets	Threats	Controls
Data	• Data breach • Misuse or manipulation of information • Corruption of data	• Data protection (eg, encryption) • Data-recovery capability • Boundary defense
People	• Identity theft • "Man in the middle" • Social engineering • Abuse of authorization	• Controlled access • Account monitoring • Security skills and training • Background screening • Awareness and social control
Infrastructure	• Denial of service • Manipulation of hardware • Botnets • Network intrusion, malware	• Control of privileged access • Monitoring of audit logs • Malware defenses • Network controls (configuration, ports) • Inventory • Secure configuration • Continuous vulnerability assessment
Applications	• Manipulation of software • Unauthorized installation of software • Misuse of information systems • Denial of service	• Email, web-browser protections • Application-software security • Inventory • Secure configuration • Continuous vulnerability assessment

McKinsey&Company | **Source:** European Union Agency for Network and Information Security; The SANS Institute

It's those kind of things. Or maybe financial services, the financial system. But just talk a little bit more about the supply chain, for example. That's one that I think in the broad conversation and the broad business public is less discussed.

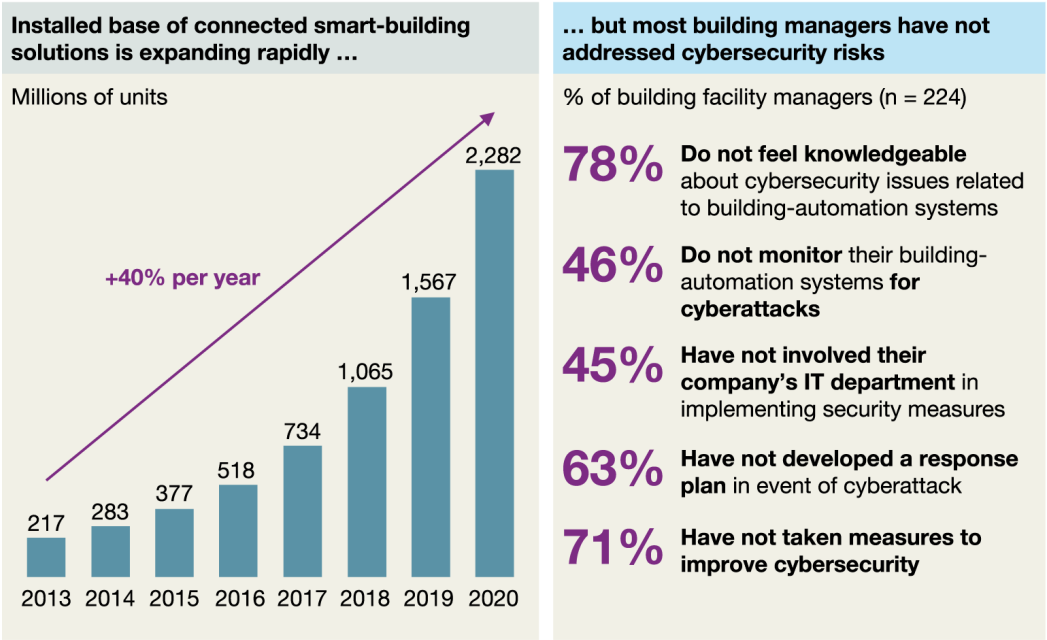
David Chinn: If you think about, at the simplest level, how a pint of milk gets onto the supermarket shelf, there are many stages in that, from the farm—by the way, the cows are milked by a machine, which is probably connected to a network—through to the transport network. The cold chain. The monitoring of the cold chain.

You don't need to disrupt anything except the record that says the milk was kept cold for it no longer to be a product that can be given to the public. The integrity of that data is the essential glue that sticks it all together.

Robert Hannigan: If you think of the big ransomware attacks of WannaCry and NotPetya a couple of years ago, one of the lessons from those is that although they almost certainly weren't targeting big manufacturing enterprises in Europe, they effectively disabled quite a lot of household-name companies. They simply couldn't do business, couldn't manufacture for, in one case, several weeks. It was a wake-up call to sectors of the economy who thought they weren't a target for cyberattacks because they didn't have great IP or data that was worth stealing.

Exhibit 2

Many professional building managers are not addressing Internet of Things security threats.



Source: Gartner; IBM; smart-building facility-manager survey in *Building Operating Management,* Jan 2015

McKinsey&Company

The Internet of Things is simply connecting more processes and more devices to the internet. And it is quite striking that the level of security built into those is usually very low because they're designed and built and procured on cost [Exhibit 2]. There will probably be a role for regulation to improve the standards there.

But it does mean companies are, both through digitization and through the Internet of Things, increasing their attack surface, making it harder for them to understand the perimeters of their own networks, harder to see where their vulnerabilities are. That is a real problem for the next five, ten years.

Simon London: And is this one of the reasons that people are very interested, for example, in blockchain? The application of blockchain in the supply chain.

Robert Hannigan: Yes, I think blockchain holds a massive potential because of the holy grail, really, of having a ledger that is distributed and unchangeable and visible to everybody. That has great benefits in cybersecurity. It's got a bad name because it's used for Bitcoin, and Bitcoin has a bad name, but I think blockchain technology is fantastic.

It's not straightforward to apply, and I think there's a lot of talk about it. The application in particular sectors for particular uses is still to be developed, to be honest. But it certainly ought to be a net gain for security, and particularly for data integrity, because one of the big future

worries is it's one thing to destroy data or steal it or ransom it. To change it and undermine trust in data, particularly in financial services, could be catastrophic.

Simon London: Or, indeed, milk, which is what gave me the thought. It's a very, very simple example, but it underlines how much of the economy runs on trust in that data.

Robert Hannigan: We're just seeing criminals moving in this direction and looking at ways of looking at the corruption of data to, for example, affect stock prices. There's a huge potential there to use the changes to data, or to put out false data, to affect the value of a company.

David Chinn: Fake news is a great example. They haven't affected the integrity of the core data. They're just simply putting out noise. In the reports on the attacks of the integrity of the electoral system in the United States, in a system which is highly distributed, where different standards and technologies are used across the United States, there was clear evidence of attempts to penetrate electoral registers. You imagine changing the electoral register so that people of a certain party simply didn't appear. In the hustle and bustle of Election Day, they probably wouldn't get to place their votes. That could dramatically undermine trust in democracy.

Simon London: Robert, we're lucky to have you on the podcast today. Why don't you talk a little bit about what is the role of government in all of this?

Robert Hannigan: It's a challenge that every government is grappling with in different ways and has been over the last ten years. There are a couple of things that make cyber particularly difficult. One is cyberdefense undercuts the assumption that government can do defense for everybody.

David has spent a lot of his time dealing with government defense in a traditional sense. And you, as a citizen, expect government to defend you using the armed forces. It's unrealistic to expect government to do cyberdefense in the same way for the whole economy, because of the scale of it, and because most of what you're dealing with is outside government. Quite apart from the fact that the skills and resources just aren't there in government to do it on that scale. So that's one problem.

The other problem is that cyber is crosscutting in every sense. It is in a new domain, so it's a bit like discovering water or air. Every department, every part of the economy, is dependent on this, increasingly, as we digitize more and become more dependent. You can't really point to a single bit of government and say, "You're responsible for cyber." That was the tendency in the early days.

The answer has to be to find a way of organizing government that gives sufficient speed and command and control to deal with the pace at which digital networks work and cyberattacks work but that actually drags out the whole of government to be good at cybersecurity, because if any one bit is bad at it, the whole system suffers.

David Chinn: Robert, it's interesting what you say because in a sense, government has three challenges. One, it is an actor in cyberspace in service of national interest, usually in secret.

Second, it has to protect itself from cyberattack. And third, it has to create, at the minimum, an environment which protects the citizens and businesses of the country.

My observation would be that, at least reportedly, the UK is very good in the first. Your old institution is a world-class actor in the national interest in cyberspace. The second is quite hard, defending government, because there's so much of it.

The technical skills of government, government IT, are continually in the newspapers and in the public accounts committee as being something that we struggle to do well. Simple things, like putting a working computer on everybody's desk, let alone defending those networks.

Robert Hannigan: Most governments, including the UK, have focused their attention on protecting government networks, sometimes interpreted slightly more broadly to take in some critical bits of national infrastructure that really, really matter, but to encourage the rest of the economy to get better. So we spent ten, 15 years, in a sense, preaching at companies to get them to raise their standards.

There was quite a critical shift, certainly in the UK, about three or four years ago, where we decided that a security model that depended on everybody and every company doing the right thing all the time was almost bound to fail. The whole system was not designed with security in mind, so the people who invented the internet and then the web that sits on it didn't have security at the front of mind, and so we are retrofitting that, and have been over the last 15 years.

Things like scanning websites for vulnerabilities, which is, again, being done across government, you could do nationally, and you could make that available nationally. One of the problems, I think, is that because the internet wasn't designed with security in mind, security is seen as something you need to add on rather than something that's built in.

We need to reach a point where security is designed in and is there by default, particularly with the Internet of Things. That may require some regulation and certainly will require bits of the economy, including insurance, to start to drag up standards.

David Chinn: Do you think government's been remiss on regulation? My observation would be that GDPR [Exhibit 3], which is not a cyberregulation, but that puts significant penalties on institutions for allowing private information to be misused, which includes being stolen, is having quite a big impact already in terms of reporting and transparency, which is then going to inevitably lead to more investment and more focus by organizations on protecting that data. Do you think government missed the boat a little bit on regulation?

Robert Hannigan: I think government, certainly in this country, has been reluctant to regulate, for all sorts of reasons. In cyber, there's a particular reason why regulation can be difficult, because it can end up being very prescriptive and very tick box, and it doesn't take account of the speed at which technology is changing and the particular networks that a company may have. We preferred an advisory, "Here are objectives you should meet"—a risk-based approach, I suppose.

Exhibit 3

The General Data Protection Regulation sets out guiding principles for data protection.

Principle	Explanation
Lawfulness	Data should be processed only when there is a **lawful basis** for such processing (eg, consent, contract, legal obligation)
Fairness	The organization processing the data should provide data subjects with **sufficient information** about the processing and the **means to exercise their rights**
Transparency	The **information provided** to data subjects should be in a **concise and easy-to-understand format** (eg, the purpose of consent should not be buried in a lengthy document of terms and conditions)
Purpose limitation	Personal data may be collected only for a **specific, explicit, and legitimate purpose** and should not be further processed
Data minimization	The processing of personal data should be **adequate, relevant, and limited to what is necessary** in relation to the purposes for which those data are used
Accuracy	Data should be **accurate and kept up to date**
Storage limitation	**Data should not be held** in a format that **permits personal identification any longer than necessary**
Security	Data should be processed in a manner that **ensures security and protection against unlawful processing, accidental loss, damage, and destruction**
Accountability	The **data controller** is responsible for **demonstrating compliance**

Source: Regulation (EU) 2016/679 of the Council of the European Union, European Commission, and European Parliament

McKinsey&Company

Simon London: Best practices and these kind of things.

Robert Hannigan: Yes. Then there is a good case for saying we need a tougher approach on regulation. I think the EU is moving in that direction. I think GDPR has been a net benefit, because essentially there are two sides to most cyberattacks. There's "Did you do the right things to prevent it, and then how did you handle it afterward?"

So GDPR has been particularly strong on the second bit. First of all, it's removed the debate in companies about whether they reveal the attack and how long, because they have to. That's good. It's raised awareness in boardrooms and so, to some degree, panic in boardrooms.

But I think the best regulation probably is in the states. It's interesting to see that California is introducing some hardware-IT supply-chain regulation, which will have a big impact, I think, given that so much of it is designed there, even if it's mostly made in China. There is a place for

regulation, and we probably should have done more of it. The difficulty is lack of skills, again. I think most governments don't have sufficient skills.

Simon London: Ah, well, that was going to be my next question. Yes. To your point, David, I mean government IT doesn't have a massively positive reputation in the world at large. Sometimes unfairly. But yes, do governments have the technical skills in cyber to protect their own networks?

David Chinn: The interesting thing about cyber is that the source of innovation in attacks is mostly coming from inside governments. Many governments have very highly skilled people who when their knowledge leaks into the public domain gets adopted quickly by criminals. We have the equivalent of government weapons proliferation into cyberspace.

If you follow the cyberindustry, where there's a huge number of start-ups, effectively, each year's retiring crop of government hackers is bringing new innovation from inside the secret domains of government in an appropriately, hopefully appropriately, modified way to the benefit of those who are under attack, often from other governments. One can't say that there are no skills in government. The best skills are probably in government.

Robert Hannigan: That's true, but I wouldn't underestimate the creativity and innovation of criminal groups. They are genuinely creative. They are talking to each other about, "How could we do this in a better way? How could we defraud this particular bank? What technique is going to work best? What's the best way of delivering it?"

They are doing what so many traditional companies are trying to do, which is pull in skills from around the internet. Not necessarily colocated. They've clocked something about how to harness young innovative skills and do creative things. We have quite a bit to learn from them, I think. I agree that governments have been very good in quite a small and narrow way, but the criminal world is also pretty innovative.

David Chinn: I think this is similar, certainly in the UK, to the crisis in STEM education. If people don't study STEM subjects, we're just not going to have the inflow into the economy, whether it be for government or private industry.

I've been particularly impressed by the way that Israel has effectively said that this is a national defensive-capability issue, but it's a national industrial-growth issue. The country decided they wanted to have one of the world's leading cyberindustry platforms and that to do that they had to make a massive investment in skills.

They started with after-school activities in the most deprived areas, because they recognized that if you start young enough in a country where almost every home has a computer, even those with very low means, who think that having a computer is important, that you can build those skills, in a sense, in parallel to formal education.

Many people who are extremely talented in the cyberdomain actually don't do particularly well at school. It's an outlet for those people, and I think it's been very, very successful. It's created a great pipeline of talent into government and private industry.

Simon London: I think about another interesting question for government is how you manage this tension between the need for transparency and bringing the whole economy with you, and yet at the same time there is an element of secrecy, acting in the national interest and so on. How do you manage that tension in practice?

Robert Hannigan: I think the key insight of the last ten years has been that you can't do cybersecurity in secret. You can't do it behind a wall in the intelligence agencies. For the obvious reason that the attacks are out there in open source in the economy, on the internet. It's all visible. Well, most of it visible.

It makes no sense to try to do it in the way that you've tackled traditional security threats, which may be very, very secret and coming from very sophisticated governments. There is a side of that that is true for cyber, but most of it is not. Most of what people experience in cyber, whether companies or individuals, is crime. Some of it's state-backed crime, but still crime. And it simply doesn't work to be referring constantly to a secret world that can't really communicate.

The obvious development here has been to create a national cybersecurity center that was outside the secret world, but under the aegis and under the control of GCHQ, which is where the skills sat. And to have a blend of both. In the headquarters you've got access to secret systems for some people, but the key point is that you have openness to industry, and you have industry people sitting alongside government experts.

It goes back to our discussion of regulation. What you need in cyber, you can't simply have cyberregulators who do it for everybody, because so much is domain-specific. You need to understand the energy sector to regulate or advise on how to do cybersecurity of energy, or for any other sector. It's different. Therefore, the idea is to have experts from those particular sectors sitting literally alongside a deep cyberexpert.

Simon London: To your point, David, it sounds like a lot of companies are struggling with this same cultural pull between the secrecy but the need to share information really to be effective, or to be more effective and to collaborate with your peers and share information.

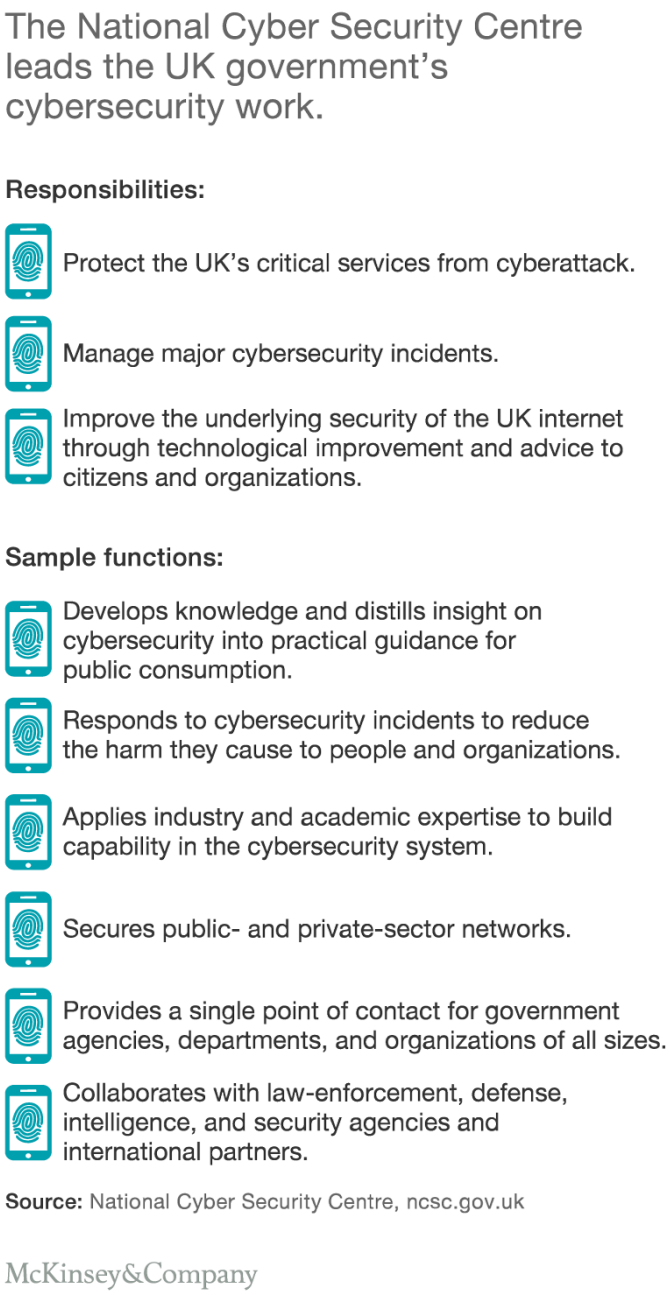
David Chinn: Yes, and I think we'll see the information commissioner shaping the environment around transparency quite actively in the very near future.

Simon London: This is your point around regulation?

David Chinn: Yes. I think that will really change people's understanding of how much they can legitimately keep secret.

Simon London: Can we just internationalize the conversation a little bit? If you look across the international context, what are other governments who are doing this well and innovatively, and who we can all learn from?

Exhibit 4



Robert Hannigan: I would say Singapore and Israel are doing it very well, in slightly different models. Australia has chosen a model that's similar to the UK model [Exhibit 4]. Having it all in one place effectively. Certainly, the operational side of cyber.

Most governments are organizing and constantly tweaking the system. There are very different models, and in Europe, perhaps in Germany especially, the cyber agencies are purely civilian. And then there is a secret-world element of cyber, and I think they're also looking at how to bring those two together in a way that works for them, given the different constitutional setup.

The military in many countries has a primacy in cyber, and certainly in Germany they've been given a strong lead in cyberdefense. That brings both opportunities, because the military always

have a lot of resources and they're very good at organizing stuff. But also challenges, because they're not used to dealing with defending banks and the economy, and it's a culture shock for them. They don't necessarily feel that's part of their remit. There are difficulties in the military.

The US, everybody looks to, but I think it's so large, with its multiplicity of agencies, that it's struggling. It has fantastic capabilities, obviously. The private sector is probably better organized, particularly in financial services, than anywhere in the world. But you often get the criticism or complaint from the private sector that the links to government are not quite right yet.

That I think reflects partly the fact that it's still evolving; the Department of Homeland Security, that was given this leadership under the Bush administration, is still developing. It's not straightforward, particularly on that scale. I don't think anybody has a perfect answer.

David Chinn: I think the military is a very interesting subset of government because I don't think there was even one model in the military. Some countries are creating cybercommands. Others are building cyber in all of their commands. Others are concentrating in their intelligence services, and then combining those in different ways. And that's also changing over time.

Simon London: It sounds like we're in an era of institutional innovation, in many ways—to some degree, institutional improvisation to try and figure out what models work in what context.

Robert Hannigan: Absolutely. I think the military's a very good example, particularly outside the US. The US is ahead of anybody, I think, in developing cyberskills in the military at scale. On the broader point about civilian structures and civilian/military, I think the one thing that is probably key is that many of the questions are the same, starting with, "What does government actually want to achieve?" And not being overambitious in what government can achieve, and what's the appropriate role of government, is a good starting point. And trying to define what people expect from their government. Things like a single source of advice, incident response, protection of certain networks. I think that is a conversation that just about every government is having in different ways.

David Chinn: But I think there's a paradox here, because if you were to interview the chairman or chief executive of any large corporation and ask them what's their top three risks, cyber would be on that top three, for every single one. And for many of them, it would be number one. Yet, if we look at what governments are doing, this is the one area of national security, of crime prevention and prosecution of critical national infrastructure, that governments have, to a large extent, abdicated their responsibility. Great, some small steps. And sorry, I don't mean to be critical of what was a big small step. But exalting the private sector to do better feels like a very different role that government takes in almost every aspect of life that would feature for most people in their top three risks. I think there's a lot more to do, but unfortunately we may have to wait for a genuine event—people talk of the cyber 9/11—to create a big change in focus, understanding, spending, and so on.

Simon London: Let me just put that back to you. What should be done?

David Chinn: What would your list be, Robert?

Robert Hannigan: Your criticism is very fair. I mean I think the government has moved from an absolutely sort of hands-off position to say, "Well, we'll look after our networks, but everybody else should get better." And sort of slightly hectoring them when they're not good enough. To saying, "Yes, there are things that we could do at national scale."

The problem, I suppose, at the risk of sort of making excuses, is that the nature of cyberspace, however defined, makes politicians feel quite impotent, because it cuts across jurisdictions. They can pass laws in their own parliament that really have zero effect. They can regulate their own companies, but not necessarily others. That is a real problem.

For cybercrime, for example, most of it is based in countries which are either endemically corrupt or unwilling to do anything about it for geopolitical reasons. What do you do about that? I mean there's a much bigger context here of international relations, and we are a million miles from getting any kind of international agreements on the security and safety of cyberspace.

Simon London: David, you were the rousing voice of critique just now. What should be done?

David Chinn: First, a sophisticated debate around the legislative and regulatory environment. The use of product liability has been very effective in other sectors for changing the game for the manufacturers. A robust thinking about product liabilities, extension to the technology arena, would frankly have quite a chastening effect on industry.

Simon London: In other words, selling a product that has technology embedded that is deemed to be insecure could be breaking the law.

David Chinn: Well, not necessarily breaking the law, but would expose you to civil action that could have severe financial consequences. Effectively, it would create a market mechanism for valuing more secure products. Second, there is room for some better and some more regulation. For example, if you want to sell anything to the UK government, you have to meet a minimum standard called Cyber Essentials. This is not the most sophisticated, but, as we've discussed, most of the attacks are not the most sophisticated attacks.

These kind of standards are very helpful because they're easily adopted by people for their own supply chains. I think a promulgation of standards, ideally with some degree of harmonization. And it's very interesting, in the US the national standards organization, NIST,[2] has created a number of models, which have got global acceptance. Once an authority puts it out there in a world where there's a lot of uncertainty, there's a lot of demand for good standards.

The traditional tools of government around legislation, regulation, standards setting, and so on could be used quite a lot more, without throttling innovation. Industry always says, "You're going to throttle innovation." What they mean is it's going to cost them more. But the cost to society of insecurity is high and is going to get higher.

Simon London: One of my takeaways from this conversation, tell me if this is right or wrong, is that there will be one or more significant tier-one, we might call them attacks, on critical national infrastructure. We're recording this in London, but it may not be based in the UK. But that will come. We know where it will come. And that will probably shift the debate into a higher gear. That probably will shift the international debate about what is to be done and, in some

[2] *National Institute of Standards and Technology.*

ways, get this taken more seriously, perhaps at government policy and regulatory level. Is that a correct takeaway?

Robert Hannigan: I think for most people, most of what they would experience, and most companies, is still crime. So that's the volume, but everybody understandably gets excited about the catastrophic attack and that there is a range of possibilities for and the insurance industry worries a lot about systemic failure. So systemic failure of cloud providers, for example. Systemic failure of some major financial institutions, two or three of which would bring down the system or could bring down the system. So those are the kind of real tier one. But there may be some political tier-one problems and attacks that will have the kind of effect that David was talking about earlier, of panic and political pressure.

Simon London: Trust.

Robert Hannigan: Yes, either trust or an attack that leads to loss of life. It might not be massive loss of life, but it would put huge pressure, as terrorism does, on politicians to react.

Simon London: So what's that Churchill phrase, this is not the beginning of the end. This is the end of the beginning?

Robert Hannigan: Well, I don't think it's even really the end of the beginning. I think we're still at very early stages of this technology. For most people, it's 15, 20 years old. Even if you look back to the ARPANET,[3] it's, what, 40, 50 years old? That's not long, and it's developing incredibly fast.

[3] *Advanced Research Projects Agency Network.*

We are about to add a massive amount of new processing power, and therefore new data to the system, mostly through the Internet of Things. We have a whole new issue emerging with quantum computing, and people have not quite woken up, including the regulators, to the fact that current encryption will cease to be useful once quantum arrives.

We need now to be building in quantum-safe encryption standards, which are available through NIST and through others. But if we don't do that, everything, every company's records, every bit of financial data, every transaction is going to be readable from the moment that quantum computing really arrives at scale. It's a wonderful innovation, and it has obviously lots of possibilities on the other side of the equation, but it is one that we need to start thinking about in regulatory terms now.

Simon London: All right. Well, I think that's all we have time for. Robert and David, thank you so much, and thanks, as always, to you, our listeners, for tuning in. To learn more about our work on cybersecurity, technology, and related matters, please go to McKinsey.com. ◻

David Chinn is a senior partner in McKinsey's London office, and **Robert Hannigan**, the former head of GCHQ, is a senior adviser to McKinsey. **Simon London**, a member of McKinsey Publishing, is based in McKinsey's Silicon Valley office.