Special Section

CYBERSECURITY & DATA PROTECTION

In This Section:

MCC INTERVIEW: Jonathan Rigby & David White / AlixPartners

A New Paradigm for Cybersecurity

Moving from protecting perimeters to a holistic system for enterprise-wide info protection

***Jonathan Rigby** has 30 years of experience at the U.K.'s Ministry of Defence, including his final position as director of cyber, intelligence and information integration. **David White** specializes in data privacy and security and information life-cycle governance. Below they discuss what companies need to understand about cybersecurity and how an agile approach creates a competitive advantage. Their remarks have been edited for length and style.*

MCC: What are the top three things corporate counsel, CIOs, CSOs, CISOs and other executives need to be worried about when it comes to cybersecurity?

White: First, my background is legal, not technical. I've always come at privacy and security from an information governance and management perspective, and I think we're seeing a fundamental shift in IT security. Traditionally, it was all about securing the perimeter and building a wall around companies to keep the bad guys out, guarding that wall, and shooting down anybody who comes over it. That approach built a culture within the IT security field that has become a little myopic. The egos of people who are concerned about anybody getting over the wall are getting in the way, and they're not accepting the fact that breaches are inevitable. The fundamental shift that we are seeing is away from the building and protecting of perimeters toward a more holistic approach focusing on how information is managed across a company and establishing programs to protect information appropriately.

This is essential because, ultimately, there are no more perimeters to protect in most environments. You could clearly identify a company's network 10 or 15 years ago. Sometimes a small number of other networks connected to it in limited ways, but they were really discrete units. Now with bring your own devices (BYOD), cloud services, major increases in web applications, remote workforces, telecommuting, outsourcing, offshoring, integration with third-party vendor networks, massive increases of sharing information with service partners and others, and even mobile and social media maps and the Internet of Things (IoT) all becoming commonplace in today's business world, the concept of a perimeter around a company is almost completely gone.

To the extent that you can define them, yes, we still need solid network detection intrusion – we still need that as a tool – but a holistic shift toward really understanding how information is created, captured, stored and moved around the company, and looking at how different people who interact with the company are accessing it, then protecting it based on its true value to the company and the true risk to the company of having it around, that's a very different approach. It has caused information security to move out of what was traditionally an IT space into more of a senior executive and risk management space. This is why we are seeing CIOs now reporting to COOs and CFOs and even to their general counsels in many instances.

A medieval castle is only going to channel the bad guys, not deter someone who really wants to get into your data.
– Jonathan Rigby

MCC: So this shift is completely realigning the internal structure of businesses?

White: Exactly, and because of that, the entire approach to cybersecurity is changing, not only focusing on system protections as a whole but other areas too, those that were traditionally not part of that information security domain. Legacy data cleanup, for example. A lot of breaches have occurred that weren't people getting into the enterprise mainframe databases of the company but stealing spreadsheets and documents that were sitting out on company group shares for five or 10 years that nobody even knew were out there – old information sitting around that nobody's paying much attention to anymore, or even old servers that were retired a long time ago but are still sitting connected to a network somewhere but they haven't been patched in a long time because nobody really uses them or thinks about them much.

Identifying that information and cleaning it up can not only save a company a ton of money in storage and maintenance but also can reduce risk quite a lot just because there is no old, unused data out there in the first place. A lot of services we have traditionally offered in that regard weren't really sold from a data security perspective – data cleanup was considered IT improvement. Often through working with legal counsel to reduce cost and risk in e-discovery, it becomes apparent. The less information you have, the less you have to discover when a lawsuit hits. Now it also has a huge impact on IT security as well.

MCC: David touched on the advent of BYOD practices. Jon, what do you foresee as the challenges related to BYOD and the erosion of the perimeter moving forward?

Rigby: I take a somewhat different approach. IT is a business enabler, whether it's enabling people to work from home or enabling payment companies to offer services through Apple Pay. And if it's not enabling, it's not actually doing what the business needs. The need to make it easier for people to work is critical. Bring your own device is only one of those extremes, but the bottom line is that if a company has data that is valuable, it has to identify the data and protect it. Therefore, if the employee is accessing that data via the corporate network through his or her own device, it's almost a strategic decision as to whether that BYOD is allowed. And if it is allowed, then it's a matter of what data can be accessed by that device and reinforcing those rules with HR policies and technical controls. It's a bit like remote working or people using memory sticks; at some stage you've got to absolutely decide what's allowed and then lock it in. It is as important as financial probity and so it requires executive focus.

If you want to send an email to your executive assistant, then actually BYOD is fine. If

Continued on following page

Jonathan Rigby
A director in the London office of AlixPartners.
jrigby@alixpartners.com

David White
A director with AlixPartners' Information Management Services practice in Los Angeles.
dwhite@alixpartners.com

Continued from previous page

you want to access top client data or financial data, then clearly it's far more and probably too risky, irrespective of how much protection you put in place.

One of my experiences in government was trying to patch up the damage post-theft by insiders, and that related to making sure that people weren't getting access to data that they weren't allowed to, whether that's giving information to the individual, segmenting their work or blocking particular machines. You've got to work out what's important and put appropriate protections on it. Take a medieval castle: That's only going to channel the bad guys; it is not going to deter someone who really wants to get into your data. That's when you need a strategic approach to what you're doing. It's when you need to consider cyber defense as a battle against an opponent, not technology.

MCC: Beyond the obvious protection of consumer data and intellectual property, what cybersecurity concerns should most people also be aware of?

White: Certainly the Internet of Things is just another way that the company perimeter is being eroded as you start plugging more and more into the network. Many of those devices aren't even controlled by humans anymore; they're communicating computer to computer, and nobody's really monitoring that device-to-device traffic. When one of those devices starts behaving atypically because somebody's hacked it and is using a thermostat to exfiltrate data out of a database somewhere that thermostats should never be, there is a new set of approaches. We're starting to catch this through better internal data analytics, monitoring information that's moving around within the company between end points or around the network, looking for abnormal or illogical activity.

So there's this shift to a more holistic approach. One part deals with information while at rest, which would be cleaning up legacy data, understanding what data needs to be kept for business purposes and then managing that data properly. The second part is understanding data in motion and how it moves around within and in and out of the company. If you have a baseline of what that activity looks like, then you can start to detect abnormal patterns, such as a CO_2 sensor or a fax machine that's moving gigabytes of data across the firewall.

There have been some shifts in data security technology as a whole, offering better business intelligence and data analytics to detect some of that stuff. There are some off-the-shelf products that do it, but to be successful, you must have a solid understanding of what a normal day looks like within the company and understand what normal traffic should look like. Since every environment is very different, it's hard to use an off-the-shelf product. It really requires people who have a data analytics and intelligence background, who can model normal for you up front and help you build a program around it.

MCC: There are essentially three buckets, three segments, of a hack: cyberspies, who want to steal sensitive company information; cybercriminals, who hold this information hostage; and cyberactivists, who just want to embarrass a company for their own agenda. What are the similarities and differences in dealing with each of those components? Do you deal with cyberspies differently than you deal with cyberactivists?

White: Absolutely. I can go back to the example I gave earlier of understanding the value and risk in the individual buckets of a company, mapping out what those buckets are and classifying that accordingly, because the classifications are going to differ depending on the actors you're defending against. What's valuable to someone whose focus is espionage, the value of trade secrets, is very different from what's valuable to a criminal or a hacktivist. For the latter, there are lots of different sources – spreadsheets and information sitting out on group shares or in emails – whereas with espionage, it's more IP and technical documentations. So how you approach that and how you value and classify that information differs greatly and requires an understanding of the true value that the information has to different parties.

The recent JPMorgan Chase attack is a good example because everybody thought it was people looking for customer names and account numbers to sell, and it turned out that it was actually individuals looking to manipulate the stock market by sending out emails to those customers with the goal of manipulating the market for profit. The email addresses of the bank's customers were the most valuable to these particular actors, not the account numbers, which is what we typically assume is most valuable. The way that we value information needs to be fundamentally changed to align with what people are after.

MCC: Now that cybersecurity is identified as a business issue rather than an IT one, how does a proactive approach create opportunities for businesses to be more competitive? What are the advantages for companies that are embracing cybersecurity and are getting it right early on?

White: We have all heard a thousand times across various articles and media reports that information is the new business asset, and if we're going to consider information as an asset to a company, then proactively protecting that information becomes a differentiator between companies, particularly given the sort of shift in many companies into storing customer information not just in a traditional sense. A bank or a healthcare facility has the records of its customers, but with the Internet of Things and the proliferation of mobile applications, the types of highly sensitive and private information that companies are now storing about their customers is exponentially greater. There's been a shift in the nature of those companies becoming information companies as a whole.

For example, many companies can know every place I've been in the past six months. They can track and store that, and that information could be of value to someone. Not that I'm anyone special, but I'm sure they have some clients who are, and that information can be extremely valuable to the right people. So to the extent that they can differentiate themselves as having policies, procedures and processes in place to protect that information, they can certainly distinguish themselves from others. We've seen it particularly in cloud storage applications: Those companies that have differentiated themselves with having much more secure storage definitely have a competitive advantage over those who haven't been able to pull that off.

Rigby: As David says, if you are in a sector like health or financial services, if you can show that you're really on it with cybersecurity, then it does differentiate you from the rest. All the players that we are working with want to be at the front end of the sector and show that they are at the top of their game by investing properly in cybersecurity. It helps your reputation if you can show that you can look after your data properly. "You can trust us with your data" – that's often a really good argument.

The other argument is if you're adopting new technologies – client cloud technologies are a really good example – and you make sure that you take security into account, then you can take a little bit more risk, creating more value. You can do it more safely because you know you're using good cybersecurity. Often what I see happen is people take that risk without making sure that they've taken appropriate cybersecurity measures to mitigate the risk. Boards and CIOs must be wise to this, and they need to ask key questions about whether the risk has been mitigated. However, if you seek a competitive advantage through top-end cybersecurity and get it wrong, you can look foolish. You've got to be quite sure before you put yourself out there that you're as good as you say you are.

The Internet of Things is just another way that the company perimeter is being eroded as more is plugged into the network.

– David White

MCC: What does a corporate counsel of a global company need to present to the board regarding the cybersecurity issues that the company should be investing in next year? What type of response should the board give?

Rigby: First thing, I'd probably ask whether they understand their risk exposure. I'd also get a sense of the probabilities of a cyberattack and the potential loss, the consequences, and where those losses might fall: Reputation is one, business interruption, data loss are others. I would expect them to have an understanding of that just as they would have an understanding of financial risk – only the best firms achieve this benchmark.

Then I'd likely ask whether they thought they were investing enough in cybersecurity or information security, and I'd challenge them to a degree to understand whether they are spending enough, whether they're giving enough support to the security functions and the security team leader. Very often it's left with the CIO – who is clearly the major stakeholder – but actually it's a board-level responsibility.

Have a sense of what's reasonable in terms of HR policy or financial exposure. I'd challenge whether they feel that they're doing enough. It's difficult to decide; it takes judgment and leadership. There isn't really an accepted norm as to what reasonable cybersecurity is. I'd finish by saying – and this is where it differs to a degree depending on which jurisdiction you're in – look at whether they're paying reasonable attention to the link between national security, regulation and your own cybersecurity; multinationals will have to handle multiple, diverse requirements. Not all jurisdictions match the leading, but quite heavy, governance that exists in the U.S.

White: I'd go back to how we started the discussion of spreading your resources out in a more holistic and diverse way and not just 100 percent focusing on perimeter security, which right now is about 60 to 70 percent of budgets for malware and virus and network security. Companies should really be taking some time to do full assessments to understand where the company is on a maturity model level from a holistic perspective, not just in that isolated domain, and then taking steps to ensure that you're constantly improving that maturity level in all areas. It requires an increased focus on not just technology but on people.

We're seeing a movement out of the technology realm and into creating cultures of security across the enterprise and changing how we're approaching training. That's not just dropping a 22-page policy on everybody's desk and making them click through a half-hour training module. It is using approachable and understandable means for people to completely incorporate into their daily business activities across the company. And like I've said, understanding how data is being stored, how old it is, does the company really need it, should they be cleaning it up, what information are they sharing with other parties, what are cloud service providers really doing with their information, and getting that broader scope of understanding of how information is floating around within the company.

Continued on page 31

Forensic Road Map

Continued from page 30

want to make sure they didn't do anything nefarious before they left." This is particularly challenging because we have to make assumptions about what the custodian would have likely done and how they could have done it from their computer or email account. These investigations are interesting because we get to look at the problem holistically versus limiting our examination to a few exit points. It boils down to finding a thread and pulling on it until we get a good picture of the computer use chronology. When I look in my crystal ball for the problems of tomorrow, I would say that keeping up with exponentially growing data sets and leveraging more automation, like our AI solutions, to deal with the volume, variety and velocity is in the very near future.

MCC: Recent surveys of general counsel show that they are most concerned about cybersecurity and corruption. They want advice on how to avoid problems for their companies, not just clean up after them. How can advanced forensics help them get out in front of these areas that are keeping them up at night?

Ciaramitaro: Data is both an asset and a liability for most companies. Information governance helps us mitigate our liability by developing policies and procedures for dealing with our data in practical and flexible ways. It's important to understand your data on so many levels and create a system to protect it from those whom you don't want to have access to it, without locking it down so much that those who do need access can't get to it.

Information governance has been around for decades, and it continues to develop and adapt to today's modern needs. In short, indexing all your data sources, categorizing it into logical groups and flagging data based on the created policies is a great way to understand your data, prevent leakage and also to protect it.

Retention and deletion policies often cause an organization great consternation. There is always a fear of deleting data too soon or keeping it too long. While there is no magical or perfect solution, establishing one policy and maintaining consistency is key to gaining control over your data.

MCC: Given that you work with both in-house and outside counsel, what personal qualities have you found most important, in yourself and in others with whom you've worked, for developing the kinds of trust-based, collaborative relationships that you need to achieve the best possible results on an assignment?

Ciaramitaro: It's very important to listen to your client's needs and understand the overarching objective of the work being performed. Repeat what they are saying and confirm your understanding with them. From this deep understanding, you can develop a statement of work that will put you and your team on the right path.

The idea is to organize and establish an easy-to-follow workflow for your client and your team to use, building trust through better understanding on both sides. We never want to be a black box that only surfaces when there are problems. It boils down to communicate, communicate, communicate.

Cybersecurity Paradigm

Continued from page 28

MCC: Jon mentioned cybersecurity being more heavily governed in the U.S. What do you think governments' roles should be in security oversight, and is that different in the U.S. and in Europe? Are they evolving at the same rate or in different directions?

Rigby: Just to distinguish between government oversight and trade regulation, government awareness is probably a couple of years ahead in the U.S. than in Europe. There's no doubt that the U.S. is leading, but Europe is catching up with the regulations, and the U.K. is probably somewhere in between. But past legal, class actions seem to have shaped corporate behavior almost more than government.

White: Governments' roles have been twofold so far, and I think that's proper and appropriate. It's been laying out the baseline of frameworks saying, "Here's what we think are the best practices to create a measuring stick for companies to both properly protect information and to be able to defend against lawsuits and the inevitable issues that arise after a breach." Their other role is then to follow up and make sure a company is enforcing what they say they're doing, so when I'm sharing my personal information with company X, they're properly protecting it, and I can expect the SEC or FTC, etc., to step in and make sure that they actually are.

MCC: What other hot topics need addressing?

Rigby: People are scared about cyber and know it's important, but just trying to get their head around it and rationalizing it is difficult. What we've wanted to explain here is: Do what is reasonable, make sure the bases are covered. What is not necessarily reasonable is to assume that you can assure 100 percent protection against high-end and advanced threats. It depends what your business is as to how much you invest in that space, because you could spend whole budgets on it and still not cover everything. Break down the threat and the threat actors into groups, and then make sure reasonable measures are clear. At the top end, where it's kind of hard to get your head around what the right answer is, really have that discussion. It breaks it down into two problems, or two subsets of a problem, rather than one gross problem. I think the people staring down the barrel of this gross problem sometimes forget that there are things they can do that are not too complex or too expensive.

MCC: What is AlixPartners' value proposition in this space?

Rigby: We've got a global footprint, we've got great people, we have great experience – those three things are key. We're not going to adopt a franchise model, so if I've got a particular skill set in the U.K. that will be valuable in the U.S., that person gets on a plane and flies to the U.S. and vice versa. Some of the most valuable work we've done has been within the insolvency space, working alongside sector and financial experts. AlixPartners' small team model in which we reinforce one another's expertise really works. We've got senior people who can link the strategic piece to the technical piece.

We think critically about cyber risk and the cost of security: to be honest about that, to be practical about it and relate it to business risks, we couldn't do this in any other firm than AlixPartners.

We're experienced people, and we understand it and have great success at the strategic board level. We've done it. We've got the scars. It sounds corny, but we prefer it when the work that we are doing is tough and complex, and When It Really Matters.

Calm Before the Storm?

Continued from page 29

data transfers from France to the U.S. post-*Schrems*. In its guidance, the CNIL indicated that SCCs could be used in place of the invalidated Safe Harbor Framework until a replacement mechanism has been established. Specifically, the CNIL stated that SCCs were a preferable alternative to the use of BCRs given the time and effort required to develop and implement BCRs. The FAQs also state that, although signed SCCs need not be sent to the CNIL, it is incumbent upon organizations to maintain a copy of the SCCs that can be made available to the CNIL.

Separately, the Spanish data protection authority (the "AEPD") sent letters in early November to companies that had previously registered data transfers to the U.S. pursuant to the Safe Harbor Framework. The letters (1) informed the companies that the Safe Harbor Framework was no longer valid and thus they needed to make alternate arrangements for their data transfers; and (2) ordered the companies to report back to the AEPD by the end of January 2016 with information regarding the data transfer mechanism(s) the company had implemented to replace the Safe Harbor Framework. The AEPD's letter further stated that SCCs may be used, but they must be authorized by the AEPD, and it warned that enforcement actions resulting in fines and/or injunctions preventing data transfers may result if the companies do not provide the relevant information.

Going Forward

Although it is beginning to seem unlikely that a suitable, permanent replacement for the Safe Harbor Framework will be secured before the unofficial January 31, 2016 deadline set by the Article 29 Working Party, there is optimism on both sides of the Atlantic that a negotiated solution is possible. That said, debates concerning intelligence gathering for law enforcement purposes following the November 2015 terrorist attacks in Paris, as well as the December 17 release of the final draft of the revised EU General Data Protection Regulation, have added to an already complicated legal landscape. For multinationals doing business on both sides of the pond, 2016 promises to be an eventful and challenging year for compliance.