Episode 238: Bold Prediction Episode: Foreign Governments Will Not Hack This Election

Stewart Baker: [00:00:04] Welcome to Episode 238 The Cyberlaw Podcast, brought to you by Steptoe & Johnson. Thank you for joining us. We're lawyers talking technology, security, privacy, and government. Today our Roundup is brought to you courtesy of three great scholars and aficionados of all things cyber. Matthew Heiman, visiting scholar at the National Security Institute, formerly with the NSD (the National Security Division) at the Department of Justice. Matthew, welcome.

Matthew Heiman: [00:00:35] Thank you, Stewart. Good to be back.

Stewart Baker: [00:00:36] Yes, it's great to have you. David Kris, who ran the National Security Division at the Department of Justice. David, good to have you here.

David Kris: [00:00:44] Thank you.

Stewart Baker: [00:00:44] And Nick Weaver – The Irrepressible Nick Weaver – senior researcher at the International Computer Science Institute and a lecturer at the computer science department at UC Berkeley. Nick, great to have you here.

Nick Weaver: [00:00:58] Great to be here.

Stewart Baker: [00:00:59] And I'm Stewart Baker, formerly with NSA and DHS and hosting today's program. So we saved this story for you, Nick. We talked a little bit about it last week, but I thought it would be valuable to have somebody who could talk about the techniques involved. The suggestion – more than a suggestion, the indication – from a good paper written by a researcher at West Point and a researcher from Israel on China Telecom having hijacked a whole bunch of traffic to send it through Beijing where presumably it was inspected. Nick, how do you do that, and how serious is this story?

Nick Weaver: [00:01:45] You do that fairly easily because the basic system for Internet routing is set up with this trusted model where basically everybody trusts everybody else, and you can play very interesting games. The problem is we don't know whether these incidents are real attacks or just screw ups. There's a saying I like to use on Internet measurements: the Internet is weirder than you think, even when you include the effects of the Internet is weirder than you think. And it's often hard to tell the difference between a deliberate attack and a screw up, and some of these could just be screw ups, some of them could be deliberate attacks, and we don't have enough information to know. So the problem I have with this paper is there wasn't enough details to independently confirm because there are multiple groups that are collecting routing information all the time. And there are certain strategies that indicate an attack rather than just a screw up. And so if we had more details like IP addresses, times, we could look at these other data sources and do active confirmation of whether this was indistinguishable from a screw up or actually significantly indicative of an attack. But in any case, I find the notion that China Telecom has a dozen points of presence in the US and is a trusted BGP [Border Gateway Protocol] speaker personally rather disturbing.

Stewart Baker: [00:03:28] Questionable. Yeah. And the number of American ISPs with points of presence inside China is somewhere between zero and one. Right?

Nick Weaver: [00:03:39] Yes. But on the other hand, from China's point of view and from the NSA's point of view, it doesn't matter because a huge fraction of the Chinese Internet once it leaves China either goes through Japan, where we've got XKEYSCORE installs; New Zealand, where we have XKEYSCORE installs; Australia, where we have XKEYSCORE installs; Hawaii, where... Yeah, you get the idea.

Stewart Baker: [00:04:05] So one possibility is that these BGP hijackings are an attempt to reproduce on the cheap some of the infrastructure advantages that the National Security Agency has by virtue of US global alliances.

Nick Weaver: [00:04:23] It could very well be. And at the same time, it could be something more targeted, or it could be just honest screw ups.

Stewart Baker: [00:04:32] Do honest screw ups last six months?

Nick Weaver: [00:04:34] Yes! Honest screw ups will last six months if they don't have collateral effects. So if, for example, the honest screw up had the traffic going through China but wasn't getting hit by the Great Firewall in a way that people noticed, it's an honest screw up.

Stewart Baker: [00:04:53] And how would you suggest investigating this? Should we be investigating this?

Nick Weaver: [00:04:58] Yes, we should. What we need is we need more details on times of the events in question. And then it's a matter of looking in a couple of major data sources. You've got the BGP observatories that are looking at all of this from many viewpoints, and there are certain aspects that would suggest a strong attack versus accident. There's also people who every day map the Internet from 100-plus locations, and so they have their data going back a decade. So with more details on the events we can actually start to look and see if these look to be real screw ups or if they look to be real attacks.

Stewart Baker: [00:05:45] David, does this suggest a role for the National Security Division either in its Team Telecom capability or just as a counterintelligence agency? I assume if you wanted some of these records you could go to Team Telecom and say, "I'd like to see your records, and if you need a subpoena, here you go."

The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.

David Kris: [00:06:06] Yeah, that's right. I mean first of all, all the lawyers are going to have to get over the shock that they feel when they find out that the Internet, this grand series of tubes that they've heard about, is actually a whole bunch of little tubes, tube networks strung together. Nick Weaver knew that from birth, but some of the lawyers and policymakers will be freaking out that the dialing, routing, addressing, and signaling information that is part of the metadata that they can get with lesser forms of compulsion includes how you do the hand-off between these various autonomous systems that together make up the big Internet. And there's definitely room for investigation here. It is fascinating that China may be hijacking the seams between those little networks and effectively you know bringing their points of presence onto the North American continent and really reversing the home-field advantage that the US thought it had for years. And I would imagine there's some investigative work that could be done there to help confirm some of what this report is talking about and some of what Nick is talking about as well.

Stewart Baker: [00:07:17] Okay. Without any ability to do a segue whatsoever, I want to talk about the Supreme Court argument over cy pres – I'm gonna learn to say that, I'm going to be relentlessly a man of the people instead of using the phony snobbish "see pray" pronunciation. But cy pres came in for kind of a beating in the oral argument. But it isn't clear to me that we're going to get a decision from the Supreme Court on this.

Matthew Heiman: [00:07:50] No, it's not clear, but I will say as someone that's been on the defensive side of many class action lawsuits, both in private practice and as in-house counsel, it's delightful to see the cy pres doctrine even get aired and criticized by the Supreme Court because...

Stewart Baker: [00:08:08] The doctrine is basically – and it comes up in a lot of privacy cases where everybody suffers a buck and a half worth of damage, but there's a lot of people so you can put together a class and bring an action. And then when you settle it, you're not going to send a buck and a half to everybody, so the idea is why not give it to some charitable institution.

Matthew Heiman: [00:08:31] Exactly. And this comes up in the context of privacy class actions but also any class action. So you get to a diminished amount in that settlement fund whether it begins in a very small amount that leads to everyone getting four cents or everyone gets a big payoff. But then when you pay everyone, you get to some base amount where it becomes no longer economically sensible to keep trying to distribute it. And so what happens is class action plaintiffs' counsel say, "Oh, let's donate this to some worthy charity," which they always have some association with. That's why they're so often the "man or woman of the year" a year later by that charity because they got the remaining $3 million in that pool.

Stewart Baker: [00:09:11] And it is important to them that there be some payout because if there isn't a big payout in the direction of the plaintiffs, then it's hard for them to justify big fees.

Matthew Heiman: [00:09:21] Exactly. So this also acts as sort of a cover for them to be able to say, "Well, we know you as an individual sufferer of this Google wrong didn't get a payout, but we gave it to this worthy charity that we can all support," whatever it may be, a conservation group, a group that's in favor of greater privacy. And it's kind of a dirty little business that everyone has always put up with. But it's great to see at least some criticism from the justices on this.

Stewart Baker: [00:09:52] The justices basically – at least some of them – were saying, "What's the connection between the people who suffer the harm and these worthy institutions, some of which they may completely disagree with, like AARP?" "AARP, stop sending me that crap." And so that was the criticism that maybe this whole cy pres thing is too loosey-goosey. And then on top of that the justices started saying, "But you know this underlying case, I'm not even sure these plaintiffs had standing. How can we approve a settlement when our recent doctrines about standing suggest there's a problem?" So there's a real possibility this will get sent back to undo the case and essentially force a decision on standing, even though I'm sure Google is happy to settle it for this.

The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.

Matthew Heiman: [00:10:38] Yeah. Well, I think you know based on the reading of the case I think both parties don't want it settled. The last thing they want is detailed instructions to go back to the 9th Circuit to start digging the trench.

Stewart Baker: [00:10:51] Yep. Okay. Let's talk about something's just really you know just painful to discuss. It's a recent story in Yahoo News that suggests that the Iranians and the Chinese figured out what Internet communication systems the United States Central Intelligence Agency was using to talk to a lot of its assets in the field and rolled them all up and – in the Chinese case at least, and I'm sure the Iranian as well – summarily executed them. David, I'm going to ask you if you're willing to talk about this. Some of this happened while you were at NSD, so I won't ask you for anything classified. But how plausible is a story like this?

David Kris: [00:11:46] I only know and would only talk about what I've read in the article. And I guess I am afraid that it might very well be plausible for the CIA doing COVCOM [covert communications] just like for the rest of us. The Internet is really, really convenient and not always totally secure. You know also frankly the story about how the so-called whistleblower was treated you know will ring true at least to some observers. So I have no idea whether this is actually true or not, but it had the ring of some truth about it, and I think it does point to some larger challenges around COVCOMs and the way digital network technology has been very, very convenient and wonderful in a lot of ways. Not so great for privacy. Not so great for security either.

Stewart Baker: [00:12:43] Yeah, I have to say I'm a little more jaundiced in my view of whistleblowers. The story here is there was a whistleblower who said this is a real problem and you need to fix it. And instead of listening to him, he was moved out and ultimately taken off the contract. You know I find that when people get to litigation over their whistleblower claims, what they want is to make the claim embarrassing enough for the US government to settle, and finding a way to hitch their story to something else that is more newsworthy often is a method for doing that. So you have to take the claim that this guy was the hero of the story with some salt.

David Kris: [00:13:34] Yeah, for sure. That's absolutely right, Stewart. Everybody's seen both sides of that one for sure.

Stewart Baker: [00:13:36] Yes, exactly. So Nick, did you look at how the Iranians apparently figured this out? They caught one guy, they figured out how he was doing it, and then they went looking for other websites on the Internet that had the same characteristics?

Nick Weaver: [00:13:56] What seems to be described is basically a Web dead drop system. So every asset would have their own special site, and the Iranians found one of these apparently through a dangle or something else. And then they just basically said, "Let's find all computers on the Internet with that property." And the Yahoo story has it being through a Google search, but that's kind of relevant. That as long as there's a unique feature to a server, we can find such servers on the Internet, and we regularly do this as part of our security work. And I'd imagine the Iranians do the same thing. And once you have an identified point of communication, then it's very easy to wrap up the work. And so this is the same problem that reporters face. The first approximation is the CIA is a newsroom with a $15 billion budget, and they have the same problem. How do you communicate with sources in the face of a[n] adversary that can see everything, and once they get a lead and pull a thread and follow communication patterns? It's a really hard problem these days.

Stewart Baker: [00:15:20] Yeah, it sounds like it. And especially given the tendency toward inertia, right? It's working. There's no problem. Why should I not continue to use it? Why shouldn't I tell my buddy about it, and he can use some variation of it? But it proved fatal for US intelligence and a bunch of sources.

Nick Weaver: [00:15:39] And also the problem is you have to provide a way for the sources to communicate that non-skilled people can use. And you can't just hand them devices. If I want to communicate securely with somebody and I can do it, I'll hand them an iPhone that's already pre-configured and locked down. Unless you can do something like that, it's really hard because I have to give them some information to communicate with me in some way that still covert. And that's hard.

Stewart Baker: [00:16:15] Yeah, although if you have some idea that it might happen, you might find a way to get all of the mullahs in Iran to also communicate with websites that look a lot like the ones you use to communicate with your sources. And then they won't know who to kill, or if they do, maybe they'll get some of the bad guys as well as CIA sources. Alright. You know we've had a terrible week or two of right-wing killings and attacks or killings that were later tied in one way or another to the right wing, plus the bombs that were sent out. And that has proved fatal or nearly fatal for one of the Twitter alternatives called "Gab," not that the US government shut them down. They said they were going to continue to make their services available without censorship as long as there were no threats of violence. But the people who provide their infrastructure, such as their domain name service, said, "I'm sorry. One of the attackers" – the guy who shot up the synagogue – "posted anti-Semitic stuff on Gab, and therefore we're not going to serve Gab." And there's also a lot of talk about whether maybe Section 230 ought to be revised to say there are certain things you can't tolerate, even if you're insisting that you're not a publisher. Matthew, where does this take us?

Matthew Heiman: [00:17:57] Well, I think it's a useful reminder of what a lot of lawyers learn in law school, which is bad facts often make bad law, and I'm afraid that bad facts, if the legislators are really fixed on this, could lead to some bad legislation. I don't think changing Section 230, which essentially gives things like Twitter and Google a pass on what gets posted on a platform – they can't be held liable if I post something that's anti-Semitic or you know hate speech of some kind – I don't think changing that fixes anything. I think we get a lot of benefit from these platforms, far more benefit than harm, and so I think we have to kind of live with it. I also would point to what you just pointed to, Stewart, which is the market acted. Private market actors took a decision about Gab, which was this real rancid place for some really just nasty opinion, and it essentially is crippling it. And I'm quite happy to let the private market order itself in this fashion. So I would really encourage our legislators to continue to speak out about the speech, but we don't need to try and you know talk about what kind of speech is okay for purposes of the Communications Decency Act.

Stewart Baker: [00:19:06] So rather than having the government impose Lefty censorship, we should let the Lefties of Silicon Valley impose their own [unintelligible].

Matthew Heiman: [00:19:14] I would say let the market do what the market does, and you know if everyone's sick of Lefty censorship, the market should give an opening for some Righty censorship.

Stewart Baker: [00:19:22] Okay, well maybe so. Here is a perennial issue that comes up, which is whether the police can force you to provide the passcode to your phone. And there is a doctrine called "the foregone conclusion" doctrine that says when you're just providing information that the government was already bound to obtain, you're not being asked to incriminate yourself and therefore the Fifth Amendment does not protect you from being required to cough up your passcode. An Appeals Court in Florida says, "Yeah, that didn't apply here." Can you make sense of the doctrine and this decision?

Matthew Heiman: [00:20:10] Well, I can't make sense of the decision. I thought I understood the doctrine. And if you read that decision, it strikes me that the judges were not well immersed in this area of law. And so I struggle to understand how... In this circumstance it involves some youths that were involved in a drunk driving incident which wound up killing some of the passengers. And I think one of the passengers had an iPhone, and she clearly had an iPhone. It was a password-enabled device. She has the password. She knows the password. There's no doubt about whether the password is there and she knows it. So I would think the foregone conclusion exception would have allowed for the police to ask her to input the password and then do their search for whatever files or communications they were looking for. I think the court got it wrong. I'm hopeful that it gets to the Supreme Court in Florida so it can be corrected. I know there's another case that was bouncing around the Supreme Court I believe in Massachusetts that was also looking at this issue. As I know Nick Weaver agrees, I think Orin Kerr's got it right in this area in terms of you know the police have to show clear and compelling evidence that someone knows the password, has a password, and that should give them the green light they need.

Stewart Baker: [00:21:26] Because coughing up the password at bottom only testifies to the fact that it's your phone.

Matthew Heiman: [00:21:32] Right.

Stewart Baker: [00:21:32] And if they already know it's your phone and they've proved it, then it ought to be a foregone conclusion. And coughing up the password doesn't testify to anything. It just opens the door to collecting information that the government is entitled to.

Matthew Heiman: [00:21:46] Yeah, and if you want to be hyper careful about this, you could even come up with a scenario in which the police aren't allowed to know the password but they have to watch you open it for them. And that way you're not even giving away that your password is you know whatever it is – your birth date and your spouse's birth date or however it is you create passwords. I think the court got it wrong, and I'm hopeful that it gets the Supreme Court in Florida so they hopefully fix it.

Stewart Baker: [00:22:11] Alright. Well, I have taken a certain amount of abuse for all of those Internet-enabled vibrator stories that I talked about and the privacy implications of Internet-enabled vibrators. So I think gender equity requires that I point out that guys use sex toys, too, and they are also tech-enabled. And what I thought was most interesting about this story, apart from the fact that you can raise $50,000 on Indiegogo just by saying you're going to build a better device, is that the device now is going to feature artificial intelligence. And the story here says that an AI firm studied 108 hours of pornography, and their conclusion which is now being incorporated into the technology is: "We used quantization techniques to discover 16 distinct motions, and using these motions, we designed and evaluated a system that procedurally generates realistic movement sequences using deep learning. We quantitatively show that this system is superior to simple Markov chain techniques." I think what they're saying is we can give you a more realistic blowjob with artificial intelligence. One more thing where it appears that science is posing the risk of making human labor unnecessary. I've got to ask: Nick, what is a Markov chain technique?

Nick Weaver: [00:24:03] Markov chains are a probabilistic model where you say I'm at state X. I'm going to then go to [state] Y with probability Z. These are commonly used for Twitter bots, and for example, it would be very easy to make a Markov chain whose tweets sound very much like President Trump's. You basically take a huge amount of data, you build up this fairly simple model, and you basically start spouting words like "MAGA" in all caps.

Stewart Baker: [00:24:37] Well, if there is anything that I could imagine that would spoil the mood worse than having lines from President Trump's tweets tweeted at me or spoken to me in the course of this, I can't imagine any. But you will want to keep that definition handy because if you're ever asked during confirmation hearings to explain Markov chain to a senator, it will be important to point out that it has no necessary sexual connotation. Alright. Last story, just about. I do want to ask everybody about election security. But we're not going to be able to continue to cover every indictment of Chinese spies that comes down the pike. We had two or three just in the last week or so. David, it looks as though this is a kind of coordinated indictment plus Commerce Department sanctions case, at least one of them is. And that struck me as relatively new.

David Kris: [00:25:50] Yeah. You don't have to be a Trump follower. You could even be part of the "deep state" and believe that China is really flooding the zone when it comes to economic espionage and related forms of information gathering and trade secret theft and the like. So they're doing a lot, and it does look like DOJ and some of its other governmental partners are trying to do a lot in response. So we have charges here around stealing chip technology from Micron and aerospace technology around a turbo fan engine of some significance and the efforts to recruit employees and engineers by the Chinese. You've got civil cases being brought. You've got criminal cases being brought. It does look like a stepped up multi-prong effort to combat this, and the attorney general even announced with some modest fanfare – flanked by John Demers, the head of the National Security Division, and Brian Benczkowski, the head of the Criminal Division – a new China initiative in DOJ which just looks like some real focused attention on the issues. So there's a lot of activity by the Chinese. There's a lot of activity in response by the US government. And they do seem to be pushing a little bit on the creative front in terms of using combined civil and criminal authorities in concert.

Stewart Baker: [00:27:16] Yeah. This is unstoppable at this point. This is going to work its way through the US government and probably the Chinese government and the body politic for years. Doesn't matter who's elected in 2020. We're going to see this continue for quite a while. That was one observation. The other: I'm familiar with the company – the Taiwanese company – and it's not just some Taiwanese packager. This is the biggest chip manufacturer in the world, UMC. They're not famous because they usually get designs from somebody else and what they're good at is manufacturing the chips. They don't try to design them in many cases. But to kind of have the world's largest chip manufacturer become the sort of a bycatch for a cybersecurity prosecution is pretty remarkable and I think suggests that there is a kind of choosing sides element to this that you have to pick a side in what's increasingly looking like a serious economic and military Cold War with China. Alright. Last question for each of you: is the 2018 election going to be disrupted by foreign hacking, cyber operations. David, I'll give you the first shot.

David Kris: [00:28:52] So obviously whatever propaganda efforts have been done are more or less done since folks are voting tomorrow. We'll look back I suppose forensically and figure out how many tweets and Facebook accounts and other platforms were fake and Russian inspired or otherwise inspired. As to whether they're going to sort of trigger a power outage or blackout or actually really hack or dox election rolls, I guess I would guess no. They're probably, if they can do that, keeping their powder dry for the next presidential. But of course the whole idea of that kind of an attack as opposed to a propaganda attack is you wouldn't see it coming. So I can't be sure. I do think it's a big priority for the Intelligence Community despite what I perceive as a pretty stark lack of presidential leadership. I do think the IC is trying to focus on this and doing what they can to prevent it and deter it.

Stewart Baker: [00:29:49] So Nick, I'll let you answer that question and also say there was a story that we haven't covered and maybe we should just touch on briefly. The Pentagon actually has a whole plan of attack and has "forward placed" some of its capabilities. We don't know exactly what that means. But it appears that they're pretty proactively prepared to respond if the Russians do something dramatic. Do you think the Russians are going to do something, and do you think this new Cyber Command posture is going to make a difference?

Nick Weaver: [00:30:25] I don't think the Russians will do anything right now because what do they need? Sit back, relax, and enjoy a Democratic House versus a Republican president and all the Charlie Foxtrot that it entails. They don't need to do things like voter registration attacks to have the president call the election illegitimate and further spur things because you know he's going to. So I think they're just not going to bother. As for "forward deployed," that means pwn [severely compromise] the Russian power grid now so we can do a blackout later.

Stewart Baker: [00:31:06] Cool. If they screw with our election, they've got it coming. Matthew?

Matthew Heiman: [00:31:11] No. I don't think anything's going to happen.

Stewart Baker: [00:31:14] Alright. I agree. I think it was probably never as big a threat as it was portrayed as. And it has induced us to get ready to hit them if they hit us, and the juice is not worth the squeeze at this point. Okay. This week we're going to have a panel discussion I did at Homeland Security Week with Steve Rice, who's the Deputy CIO for DHS, and Max Everett, the CIO for the US Department of Energy. So without further ado, let's go to our panelists. So this is a great panel. We're going to have a good conversation. To my immediate right, Max Everett is the Department of Energy's CIO. He's got a long history in government IT, including some time as a plank holder at

DHS, helping get DHS off the ground. And to his right is Steve Rice, who's the deputy CIO today at DHS, also a long history in federal IT. He worked at TSA as deputy and then CIO, before that at the Secret Service. So again a long history of involvement in federal IT. And I want to start them off and ask them essentially as CIOs, as deputy CIOs, how much responsibility – I'll start with Max – do you have for the security of the DOE systems?

Max Everett: [00:33:06] Well, for ours it's really a DOE model. I'm the senior agency official for risk management, primarily focused obviously on cyber. So I do have that ownership. I've got a CISO [chief information security officer], and of course I've got a pretty good team not only at headquarters but out at our sites and labs who help with cyber. But the reality for anybody in this world of leadership is it's your head on the chopping block. So I'm the one that typically is called up to Congress to have those conversations and talk to the secretary and deputy secretary when those things are going on. So certainly in our agency we've embraced the model of sort of having that single belly button to own that and then a team below me who does the work really across the entire department.

Stewart Baker: [00:33:49] So how much responsibility do you have for components of DOE?

Max Everett: [00:33:56] So we're a little unique, probably more unique than people would like at Department of Energy. So if you're not familiar with our model, we have the 17 national labs under us. Many of you've heard of many of them: Oak Ridge, Sandia, Los Alamos, and other science labs as well. And so those are all commercially operated. So it is a bit of a unique piece in federal government. They're a little more integrated with us than contractors, but they're not directly federal. So it adds frankly some unique challenges for us. We've also got our environmental management, which is I think a $6 billion part of the department that's managing the cleanup of our legacy Cold War sites. Again those are almost entirely run by contractors. So it's a little bit of a unique challenge there. What I will say that with the department right now in the secretary's direction is that we're a single department. So he looks at the department as a unity, and we have a single mission there. And so as we look at those, and certainly cybersecurity is one of his priorities. And so I would say it probably looks a bit different than it has historically, the department, in terms of doing that. So we're working through some of those things right now to help people understand that while we have a distributed, federated model, there are going to be certain things that we're going to address as a department.

Stewart Baker: [00:35:14] So Steve, the same is true of DHS. It's very decentralized because it was pulled together with a bunch of different components stuck under a single DHS management.

Steve Rice: [00:35:28] I would use the word "federated."

Stewart Baker: [00:35:30] Federated. It was federated. Yes, of course, it was. So how do you make that work as somebody who has CIO responsibilities for the whole department?

Steve Rice: [00:35:41] So I've got CIOs at the department as well as at each of the operating components. Each of the operating components really look at the execution of the direct mission to that mission. CBP, ICE, Secret Service, and the like. Where we come together is where we have commonality: commonality of architectures, commonality of licensing agreements, commonality of legacy infrastructure to ensure that we understand that architecture. Department CIO under FITARA [Federal Information Technology Acquisition Reform Act] has governance of all the IT investments across each of the components. And when we see like-minded investors, we ensure that we collaborate across the CIO council, and if those areas happen to be within IT security, we bring the CISO council together, ensuring that we understand what is today's challenges within a federated model as well as what are those things that we can collaborate to either simplify the architecture or ensure that we have a better risk posture.

Stewart Baker: [00:36:33] So the Department of Homeland Security has started issuing binding operational directives [BODs]: get Kaspersky out of your system, DMARC [Domain-based Message Authentication, Reporting and Conformance]. Let me ask Max since he's not responsible for them: How's that working? How do you think the BODs are actually functioning?

Max Everett: [00:36:54] Well, look I'll be honest with you. I'm a bit of a fan of the BODs for a few reasons. One is I think there are some things we should be doing as a federal government. Second for me is because they are in fact binding; they're legally binding. They do apply even to my contract labs. If they have federal infrastructure there, as they often do, that applies there as well. So those are things that we have applied you know when you look at Kaspersky, when you look at BOD 18-01 ["Enhance Email and Web Security"] (DMARC and those things), we have applied those across the entire department. And so I think that's important in that it's real. For me it's you know when I look at again where I would go – we're beyond federated, we're confederated – and so when I take the step back, there are things like that that apply across the entire department that help us have a little bit of unity of effort, and there are things that any particular lab or smaller program – they might not say that's particularly important, but looked at a departmental and federal level, we have a level of stewardship that goes beyond any of our sort of day-to-day mission requirements. And I think the BODs are made to reflect those.

Stewart Baker: [00:37:59] So DHS I assume has fully implemented...

Steve Rice: [00:38:03] Absolutely. You know I take a step back. I mean if you think about it, it really harmonizes risk. So you can look at it from a department perspective or a full USG [US government] perspective. It allows an understanding of what are the risk objectives for an organization, and a binding operational directive allows you to prioritize work.

Stewart Baker: [00:38:21] So the problem I see with the BODs is they are very kind of single-focus demands. Right? "You shall do DMARC." That is not a complete security solution. It's just a spot solution, and even more so, "get Kaspersky out of our systems." Is there a way in which the BODs can migrate to something that's a little more systematic?

Steve Rice: [00:38:48] As this process matures, I think you'll see a change in thought of how to make sure that you can harmonize these and make sure that you have a well-orchestrated outcome that these BODs will take us into that direction.

Stewart Baker: [00:39:01] So thinking about security of federal systems, what differences do you see between the security measures and approaches and needs in the private sector and the sorts of things that you have to do for a federal agency? As I know I'm going to assume that 90% of it is the same. But where's the 10%?

Steve Rice: [00:39:25] I've got to be honest. One of the most enjoyable conversations I ever had is with the CIOs of private sector, and the world is not that much different. What I like to do is I like to understand how are they delivering services, how are they looking at risk, how are they understanding where they make trade-off decisions. I consider the organization at DHS highly regulated, whether that is for NPPD [National Protection and Programs Directorate] across the federal CIO council, whether that's with my leadership, and where we look at this is articulating how a federated operating model is different in a lot of degrees than private sector.

Stewart Baker: [00:40:01] Do you think the private sector is less federated?

Steve Rice: [00:40:03] It is less federated to a greater degree than I think the Department of Homeland Security. So we diverge a little bit in the responsibility of the department CIO to ensure that they have collaboration across each of the components. And what I have seen is within DHS at the department level it's the width of the mission. If you're operating CIO at CBP, ICE, TSA, or the like, your day is driven by that execution of that mission. DHS, it's the width of the mission. Every 30 minutes you can be in a different meeting, whether it's immigration enforcement, cybersecurity, finance acquisitions. And that's what really changes the risk aperture between a component

CIO, private sector CIO, and a department-level CIO is understanding and appreciating that level of risk.

Stewart Baker: [00:40:49] So Max said you also have the federated approach. Let me ask this. I agree the private sector tends to be much more single office responsible for providing everything. Is it possible that that's really the right solution and that government because of the way government works and the responsibilities to particular stakeholders has saddled itself with systems that will always be federated and therefore much harder to secure?

Max Everett: [00:41:20] Well I think if you step all the way up, even to the National Cybersecurity Strategy, you see there's – if you've read through that – you'll see there's an effort to start looking at going back to what you said start to take things like the BODs, make them more strategic and more systemic across federal government. So I think people in fact have recognized that. I got to spend some time in private sector, and as I look at Department of Energy, there is really no comparable – you know we are about $30 billion entity, and you know we'd be in the Fortune 100 – there is no real comparable entity, even if you look at large conglomerates. There are no large conglomerates that are both highly regulated but also have that breadth of mission. Any private sector coming at our breadth of mission would have spun off the different pieces many years ago.

Stewart Baker: [00:42:08] Yeah, and you would've gotten equity!

Max Everett: [00:42:08] Exactly! That would have been better. But I worked with private sector companies, and they may have lines of business. Right? I think the big advantage I've seen if you're out in private sector is two things. One of course is you've got that ultimate metric of money. You can look at profit loss. The second thing of course is I believe because the way most companies do their finances, they can actually do life cycle planning for their delivery of mission systems in a way that we – we are subject to the way that the federal government budget works. And you saw, even if you look at for example, the Technology Modernization Fund [TMF] in the MGT

[Modernizing Government Technology] Act, a lot of people focused on the money out of that. But the other half of that I think is actually more important in that the purpose of it is the idea of doing a working capital fund that reports to the CIO. And the point of that is not to build little kingdoms for CIOs. The point of that is to actually build a mechanism where we can do life cycle planning. Right? I joke, but it's unfortunately a true joke. Most of us in government, we build a system. We wait three or four years. We realize the system is now out of date and needs to be updated, and only then do we actually go look for the capital that we need to do the update. But then we get stuck in a CR [continuing resolution] for a year or two. So now we're throwing money back on a legacy system that's not delivering mission capability. And it takes us another two years to get the actual capital to get a budget to get the capital to do the upgrade.

Stewart Baker: [00:43:32] So somebody just gave me a bumper sticker that says: Building the Legacy Systems of Tomorrow. So let me ask about the move to the cloud because that addresses in a lot of ways the capital problem. You're now renting space, and you don't have to go out buy machines. It's odd that MGT came along just as we started to have less need for these big boluses of capital investment. Do you see the move to the cloud as an opportunity for security or an opportunity for insecurity?

Max Everett: [00:44:15] Well I've always looked to the cloud – I'm very much a proponent of it. I think the important thing about cloud is it's not more or less risk. It's different risk. That's all it is. And so to say that it's more or less secure is a misunderstanding of security. You know there are different things that you have to take better ownership of. It's really for me I think around change management and access controls. To the degree you're doing those well, if you're not doing those well in your internal environment, you're going to be just as compromised in different ways. It's probably a little more public in the cloud, but those are things you have to do well, and if you're doing those well, you know the cloud... And again I think the other thing that I've tried to work with our folks as a department to step back on is: we talk about cybersecurity is this discrete risk; it's a part of broader risk. Right? There's mission risk. There's financial risk. There's all these other risks that are part of that. If my folks can't do their job, if they can't perform mission, that's a risk because I know what they'll do:

the same thing they do in private sector. They'll go get their own credit card, and they'll go buy cloud on their own. They'll go buy something on their own. They'll use their own budget authority to get something on their own, slip it by us where we don't get it in FITARA. And to be fair, I don't blame them. They're not trying to undermine us. They're trying to get their mission done. They're doing what they're incentivized to do. And so to the degree that we're not keeping up with them, they're doing what I would try to do if I was in their place. And so we're trying to move ahead and do that, and our labs frankly have moved far ahead of us as a department on getting the cloud and taking advantage of it. We're trying to catch up now on some of our federal systems. That was some of our work with the TMF fund and other things to try and get out more quickly to the cloud and then – and this goes back to something you said, which is – then get a bit of a more holistic view of how we look at risk and risk management across the department. And so my job as CIO is to set a bit of a platform and a standard. I have some labs that should be taking more risk. And of course I have, for example, our nuclear labs who should take much, much less risk. But if we set a bit of a baseline, we can have those apples to apples discussions.

Stewart Baker: [00:46:19] Steve, how do you work with the components on the cloud? Are there components at DHS that have started to make that move in a significant way?

Steve Rice: [00:46:27] I tell you that cloud is forcing a lot of conversations at the Department of Homeland Security. One is, you know depending where you sit, some people think there's only one cloud. So there's a level of conversation about what is the cloud, what is that architecture, what does that mean. When we start talking about cloud, it really forces you to start thinking about your transport layer because if you look at it, we have mission executions that are very austere conditions. So the insurance of how do you transport data wherever those cloud compute centers are going to be, how do you ensure you've got the latency, you were identifying that and treat that accordingly. Additionally, not everything at the Department of Homeland Security has is going to the cloud. So understanding rationalization of applications: what's going, where do your investments [go], where do you start building momentum, what are the easiest things to move first, are those things you'd have to look at some level of investment?

And you know we talked about this a little before, but it's much like moving your home. And when I bring this up and everybody starts nodding at me strangely. It's when you move, you're going to go through what you're going to take to the new home. You're going to get rid of those things that are duplicative, those things you no longer want, and you're going to make sure that you kind of scale down a bit. That's rationalization. Number two: whatever you're going to take new home, you're gonna put it into a new box, you're going to label that box. You understand your inventory of what you take. So what it allows us to understand is when we move to that new environment, whether it's an Azure, AWS type environment, we understand what our application architecture and application inventory looks like. And then it forces a common discussion about what is the underlying necessity to have that workload in that environment. Because at the end it allows us to start talking about analytics, and if you're gonna start putting these workloads, we might want to make an understanding of how do you want to analyze the data in the future.

Stewart Baker: [00:48:09] So one of the things about the cloud and moving is it's a lot easier than you might like it to be to leave the box of your most valuable stuff out on the curb. And so how do you deal with the new ways to screw up in the cloud?

Steve Rice: [00:48:27] Well, one of the biggest mistakes you can make is making sure that you don't take into account the training of your workforce, and that's whether your contract staff or your federal staff because at the end of the day, for those that are long-time feds, they may not have as much experience so you're going to have to retool your workforce to a greater extent. You have to start understanding succession planning as people start moving out and trading out of the organization for retirement. We make sure that these new skill sets are coming in. There's a dialogue and engagement with the chief human capital officer to make sure you understand succession planning and that succession planning is not based on age of the workforce but new skills and talents that need to come in as you start looking at new technologies. And then finally there needs to be an understanding of the width because when you start talking major cloud environments, you start talking about different instantiations and then you start talking about infrastructure and SaaS [software as a service] and paths and where you're going to go. It can get very wide. And one of the challenges is making sure that your training portion is understanding how are you training your workforce to work with the monitoring tools to make sure that you can work and manage those workloads. Because if you do get too wide, if you don't take that in consideration, you start making mistakes. And what I find is the mistakes are the most difficult to identify because you really didn't know that you made this mistake in the first place.

Stewart Baker: [00:49:41] Right. And then it can go on until somebody embarrasses you. Yeah. So Max, you said a couple of times that you're in a highly regulated environment, and I think that does make sense. Not only are you subject to a variety of regulations and passing regulations on to the labs, but DOE's responsible for regulation of cybersecurity in the energy and nuclear facilities that are among the top targets. First, how do you work with the people who are responsible for regulating cybersecurity there, and what are the adversaries you worry about the most?

Max Everett: [00:50:26] Sure. So the way we work with them is we do – again and I will say that DOE, we ourselves, are not the regulatory entity, which is great for us because it allows us to have a little more open conversation. We work very closely with NERC [North American Electric Reliability Corporation] and FERC [Federal Energy Regulatory Commission] who are the regulatory entities. You know again we have very close relationships with them across a number of sort of layers in our department. So our role – this is one of Secretary Perry's priorities. It was enough of a priority he created a new office called CESER [Cybersecurity, Energy Security, and Emergency Response], and it's basically taking some of our existing work on cybersecurity research in the sector, our emergency response function – we just had one for a hurricane – putting those all into one place where there was sort of a single belly button. We've got a new assistant secretary there. And so I work closely with her and our assistant secretary on resilience as we sort of put together how we work with the sector. We actually have the electric sector coordinating council. We just briefed them the other week at our headquarters. We work closely with IT-ISAC [Information Technology - Information Sharing and Analysis Center]. So again very similar to what – we do as a sector-specific agency, but we do it in coordination with DHS which does it across you know any number of these sectors. And so it's much like what they do. It's building relationships. I think one of the very unique things most people don't know about DOE is we have in MCs called the power marketing administrations. Those are – they're pretty old, they're 50-60 years old in some cases – they essentially exist to resell power from federal hydro. So think Hoover Dam, especially up in the northwest the dams on the Columbia River. So they actually provide electricity as a reseller to probably over 30 million Americans, and they're actually a big part of stabilizing the grid up in the northwest. So the value for us is that gives us a really unique insight into – as we work with our regulated friends in the private sector the in the electric industry in energy – it gives us a bit of a unique understanding of that because we have a regulated entity. Right? They're both regulated by me, in a sense, through FISMA [Federal Information Security Management Act], and things like that, but they still report through FERC and NERC and all the requirements they have as well. So it's given us a bit of a unique perspective on that as we then go out. Then we don't just sort of throw things out there to the sector. They know we actually understand a little of it.

Stewart Baker: [00:52:45] So I'll ask Steve to join us in that. The thing that is always the biggest problem when you're trying to regulate cybersecurity is you get compliance, not security. And people say, "I've got to check these boxes. I don't know whether it makes me more secure, but I know I have to check the boxes. And then I'll worry about cybersecurity later – or never." How do you overcome that spirit?

Steve Rice: [00:53:10] Looking across just the internal to the department is understanding you know the changing in philosophy of how you understand risk, how you understand risk at a lot of different levels: the financial risk making sure that you understand how to take legacy debt out of aging infrastructure; looking at the risk associated with the contract strategies to make sure how are you staying abreast or how are you keeping those vendors to stay current on their patch management, making sure that they bring highly skilled talent to manage workloads; and then finally looking at just do research and development to make sure how are you staying abreast of the technical road maps of some of your key providers. And so understanding the ecosystem in which we are in. We're a big Microsoft shop and a big Oracle shop and a big IBM shop, an Adobe shop. How do I understand where they're making investments of where I'm going to follow those road maps? How do I influence those road maps to make sure they understand how they're taking my mission responsibilities into account? And then also having enough of a dialogue to say when you're going to move off of those road maps because some of the investment strategies just don't make sense with the department in all cases.

Stewart Baker: [00:54:18] So thinking about ways to build a more security-focused, rather than compliance-focused, solution, one of the ideas that is getting quite popular in the private sector and to some degree in the government sphere as well is bug bounties. What's your thinking – I'll start with Max – on bug bounties for DOE?

Max Everett: [00:54:45] So we are actually looking at that. My hope is in a few months we're going to be ready to roll something out. We're trying to do it in a very focused manner, but I would say the good news is as I've talked to folks at DOD and other agencies who've had some good success with this because starting with a very focused area – don't just sort of do everything, pick some focused areas. People I think have built some very good frameworks around how to do and manage that. But it does give you the reality is there are a lot of sort of the – I'll use "hacker" in its original non-pejorative sense, which is people who simply like technology for technology. Some of them happen to also care about their country. And so the idea of enlisting their help to try and secure things – I think we've already seen some successes in government. We're looking to pick that up as well because I think there's some value there, and if you do in a focused and targeted way, I think it can absolutely bring value.

Stewart Baker: [00:55:42] Steve?

Steve Rice: [00:55:44] If you look at the bug bounty, it's almost like a federated pen-testing strategy.

Stewart Baker: [00:55:48] Yes, it is. Cheaper too.

Steve Rice: [00:55:51] How do you bring people in here to tell you information you don't know about your systems? Like DOE, we were exploring it as well, understanding how we get best practices, looking at a lot of models over at DOD, and then say how do we manage this. But it's the right strategy so you can identify risk to a greater degree than we presently have today.

Stewart Baker: [00:56:11] So to make that work you usually have to have already a vulnerability disclosure program so that when people tell you they found a vulnerability, there's somebody who says, "Okay, my job is to figure out whether this is true and to figure out how to fix it and to respond to the person who disclosed it." Because if you don't have that, then there's no point starting on the bug bounties. And are you implementing that first? Is that your plan? Are individual components going to implement that?

Steve Rice: [00:56:43] No, it won't be individual component. It will be from a department perspective. But you don't want to rush into it. So you understand this work and you have some level of exposure where you can allow people to start providing that information. How do you properly resource to make sure that you're communicating as well as whatever vulnerabilities identified that you can remediate them in a timely fashion, and then three is learn from those lessons. So how do you want to expand over time? So you have a recurring, expanding program.

Stewart Baker: [00:57:09] So Max, the thing that would make me most nervous if I was sitting in your shoes thinking about bug bounties is IoT, industrial control systems running power plants. They never shut down. They can't shut down. It's a disaster if they shut down for five minutes. And so saying, "Sure, why don't you try hacking this and telling me what you find," is a moment of considerable fear. Is there anybody who's doing that successfully now?

Max Everett: [00:57:41] I don't think there's anybody doing – if you have that much exposure to your IoT systems, I think you probably got a bigger problem to start with. And having worked in some of the control systems areas, the reality is the vast majority of people who are doing these things, they're used to doing IT systems. For folks who've done the pen-testing and those kind of things in an OT [operational technology] environment, that broader environment, that's different. What's the first thing you learned IT when there's a problem? “Did you reboot your computer?” That's literally the absolute, there has to be something on fire, answer when you're in an OT environment. It's completely different. So this a little of that training element, and we're going through that right now because we have OT not only in those power marketing administrations but almost every in every organization now on physical security in other areas is starting to integrate some type of operational technology. Unfortunately, sometimes we don't know that we've integrated it. Somebody has integrated it into us without our knowledge. And so that's a training element we're having to start new across everybody who does sort of cybersecurity response is to understand the difference there that you can't just say, "Oh, I'll unplug it and see what happens." That's usually never a good thing on operational type of technology. That would probably be a good ways out for I think anybody who's working in those kind of areas.

Stewart Baker: [00:59:00] Sounds right. Okay. Max, Steve, thank you very much.

Max Everett: [00:59:04] Thank you.

Steve Rice: [00:59:04] Thank you.

Stewart Baker: [00:59:06] I promised everybody that I would try to spur more reviews of our podcast and that I would read some of the more entertainingly abusive. So here's one from “Nick of Steel,” who reviewed us on Apple podcasts: "Stewart Baker is less funny than he thinks" – that would not be hard – "and substitutes snide political asides for analysis. I guess he's playing to Steptoe & Johnson's client base. As a podcast, however, it would be greatly improved by a humbler, inquisitive host." So that's not bad, but it's not that funny.

David Kris: [00:59:48] Was it Nick Weaver submitting that?

The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.

Stewart Baker: [00:59:52] It must be! Yes! He does spell it the same way, so maybe what he's suggesting is that he could be the humbler, more inquisitive host.

Nick Weaver: [01:00:02] Oh, hell no! I'm not humble!

Stewart Baker: [01:00:07] [Laughter] Well, that is the problem. Anybody who's willing to do this probably isn't humble enough for “Nick of Steel.” Okay. Please do send in reviews. If you think you can beat that, beat that. I'll take almost any abuse for a five-star review, and I will read it on the air. If you think that was unfair and you think that I am as funny as I think I am, please submit a review to Apple so that others can read both sides. Send us your thoughts for additional guests to CyberlawPodcast@Steptoe.com, and we'll send you a mug. Join me, @StewartBaker, on Twitter and you can see a little advance peek of what stories we're thinking about using for the week. We've got a bunch of good guests coming up. I did a deep dive with an ABA panel of luminaries on CFIUS. We'll be turning that into an interview. Mieke Eoyang of the Third Way is going to talk about some pretty interesting cyber enforcement ideas that her institution has come up with. And Representative Jim Langevin, the most well-informed Democrat in the House on cybersecurity matters, will be talking on the cyber work that he has been doing in Congress, and by the time he talks, we'll know whether he's going to be in the majority or not. Finally, show credits: Laurie Paul and Christie Jorge are our producers; Doug Pickett's our audio engineer; Michael Beaver's our intern; and I'm Stewart Baker, your host – almost as funny as I think I am. We hope you'll join us next time as we once again provide insights into the latest events in technology, security, privacy, and government.