Focusing On The Future: Prioritizing Security in the Digital Economy

TECHNOLOGY

THREAT

TRUST

November 18, 2016

Washington, DC

THE CHERTOFF GROUP

Event Summary

KEY FACTS

150 Total Participants

27% C-Suite

47% Government/Tech Industry

"I found the event to be very enriching and providing great thought leadership. I really liked the format with very few PowerPoints and more discussion. Be happy to participate in future efforts"

– Speaker

"This was an event I consider one of the best I have attended in this past year. The content and speakers were excellent. Also it allowed for ample time to network with others who have similar goals."

– Attendee

Table of Contents

Sponsors

COALFIRE

CISCO

Microsoft

LANDESK

SailPoint

Event Partners

Passcode From The Christian Science Monitor

THE CIPHER BRIEF

Executive Summary

In today's digital economy, developing and prioritizing a cybersecurity strategy is critical to address diverse and evolving threats, foster trust in the technology we use, and define a path forward where security is seen as a business enabler. More executives need to understand that cybersecurity is essential to their digital strategies and for the creation of lasting competitive advantage.

With this in mind, The Chertoff Group Security Series convened 150 leaders across government and business communities to discuss critical policy, technology, and risk management issues that will be shaping the security agenda in the near term. Experts shared their unique insights around the fundamental question: "*Moving forward, how do we prioritize security in a digital economy?*"

With an overarching theme of "Focusing on the Future: Prioritizing Security in the Digital Economy," The Chertoff Group Security Series framed the conversation around the "Three T's" - technology, threat and trust. These big, interrelated ideas have a profound impact on strategy, policy, and public opinion and are critical for everyone to understand – whether you are a business leader, policy maker, investor, or entrepreneur. When done correctly, technology and policy can be a fuel for digital transformation and growth but when done incorrectly can be an inhibitor to the same. How can today's leaders leverage technology, react to evolving threat, and shape trust to improve their resiliency to risk, build competitive advantage, and accelerate growth?

Jim Pflaging Head of Technology Sector and Business Strategy Practice, The Chertoff Group

The 2016 election ushers in new leadership that will shape policy and program initiatives during the "golden age of innovation," which is profoundly changing the economy through technology-driven tectonic shifts including open source, social media, big data, cloud, mobility, and the Internet of Things.

Unfortunately, this golden age, has enabled a new class of bad actors to take advantage of security vulnerabilities in these platforms, creating new risk in the form of cyber threat – the "Second T." Emerging technologies have created a digital environment that has triggered a series of new security risks facing both government and private enterprise. To combat the emerging cyber threat, the next administration must bolster public-private partnerships to ensure the development, promotion, and use of cybersecurity technologies, polices, and best practices.

The ongoing occurrence of security breaches during this election cycle and beyond have contributed to an ongoing erosion of trust, the "Third T." You could argue that we are living in an unparalleled age of uncertainty. The concern over security and privacy is more prevalent than ever before. Industry and government must collaborate to build a more secure environment, mitigate risk, and build the trust that citizens have in government and consumers have in business. Trust is fundamental to sustaining growth while properly addressing security and privacy concerns.

Many business leaders now recognize that cybersecurity is more than a technical risk, it's an enterprise wide risk, and often their top business risk. In today's digital economy, you simply cannot have an effective digital or growth strategy without a tightly interwoven cybersecurity strategy. Security is now being perceived as a competitive differentiator and will continue to be a market distinguisher as technologies and threat continue to evolve in the years to come.

Across keynote and panel discussions, expert speakers and industry thought leaders addressed the impact of the election on the future of cybersecurity, innovative ways the public and private sector are tackling cybersecurity issues, and how enterprises and boardrooms are increasingly addressing cybersecurity not solely as a risk – but as a growth enabler.

The following report offers a glimpse into these discussions. A full video of each discussion is also available from The Chertoff Group's website at **www.chertoffgroup.com**.

We hope you find this report insightful and thought provoking as we consider the unique opportunities now available for government and enterprise leaders as they seek to build more resilient enterprises and navigate the risk management issues that will be shaping our security agenda in the years to come.

Moving forward, how do we prioritize security in a digital economy?

Session Summaries

Michael Chertoff Fireside Chat

As former Secretary of the U.S. Department of Homeland Security and now Executive Chairman and Co-Founder of The Chertoff Group, **Michael Chertoff** is very familiar with today's security environment and the broad range of issues – from risk identification and prevention to preparedness, response and recovery – that are facing both government and private enterprise. At The Chertoff Group, he provides high-level strategic counsel to help companies grow and secure their enterprise in an environment where technology, threat and trust are shaping the way we operate.

Katy Montgomery, Managing Director at The Chertoff Group, joined Michael Chertoff on stage to discuss the role security is playing in today's digital economy and how he views many of the prominent security topics making headlines today including the intersection of privacy and security, identity authentication and authorization, encryption, and where the public and private sector can do more to mitigate risk.

Speakers:

Katy Montgomery, Managing Director at The Chertoff Group

Michael Chertoff, Executive Chairman and Co-Founder of The Chertoff Group

Montgomery: How do you view security and privacy in a digital economy?

Chertoff: In many ways they're the same thing. Privacy is about being able to maintain the confidentiality of your information and the ability to maintain trust in transactions and things that you do in your business. That's the same thing security is about. Sometimes privacy is about the promises that we make to customers, employees, or other stakeholders about how we're going to treat their information. But the promise is worthless if you don't have the capability to execute on it, and that's where the security comes in. I would say that one of the lessons we've seen over the last couple years is that even things you don't think of having business impact turn out to have enormous business impact if they are disseminated publicly. That really has an impact on the efficiency and trust you need to run an organization. I think we need to get to the point that we really view security and privacy as two sides of the same coin, and very much interrelated.

Montgomery: In terms of cyber defense, do we see more maturity and consideration for what companies can do to have stronger active defense postures?

Chertoff: From a liability and operational standpoint, there's a lot of upside if you're operating within your own network. But when you start getting outside your network into someone else's network to carry out either reconnaissance or, even more significantly, destruction or change, you're getting into a sticky area for a private party. You may be breaking the law. If you wind up at the wrong server or with a server that has been taken over by a malicious actor but is in the meantime running hospitals and schools and you take that server down, you may cause enormous amounts of collateral damage. And now you'll be responsible not only for virtual damage and but actual people may be getting hurt. So my view on this is you don't want to try this at home. The government ought to own the responsibility for that element of defense that involves offensive operations. There is some discussion about whether under government supervision private parties could be enlisted to assist in that process. But it would have to be with the authorities of the government and the guidance of the government because we don't want a private party to start a war. So I think there's a domain for private action, there's a domain for government action, and there may be an overlapping area where the

two can work together on building up our capabilities.

Montgomery: How do you see the debate on encryption? With new leadership coming in, how do you see this evolving?

Chertoff: I am all in favor of having government being able to use whatever skills it has to find out what bad people are doing. And I can tell you having worked for years in trying to detect, track, and frustrate terrorist attacks, frankly there's a lot more data and there are many more tools out there now that allow the ability to detect and frustrate attacks. On the other hand, I don't know that the solution is to weaken the defenses and security that the average innocent American has to protect their data. Because then, while you're making it easier for the government to crack into encrypted data held by bad guys, at the same time you're weakening everybody else's defenses against those very same bad guys. And I think in the end that is too high of a price to pay. So if the government, on its own, can find a way to get data, they should do it. But I don't think we should be building backdoors or vulnerabilities into our encryption systems because that's simply going to open it up to adversaries, whether they be nation-state adversaries or criminal adversaries. And that I think is too much of a tradeoff. So I think this debate is going to continue, but I think at the end of the day, the number of tools that are available to the intelligence community and the law enforcement community, even with strong encryption, dramatically increases their capabilities over what was the case twenty years ago. And so that makes me all the more confident in the view that we ought not to weaken encryption in general – which is, I think, the most powerful weapon many of us have in our businesses and in our private lives privately to prevent online predators from getting our stuff.

Montgomery: Unfortunately, this debate on encryption is circled around one particular incident and overshadows the level of cooperation that actually does take place between technology companies and law enforcement every day. Are there areas of common ground between the tech community and law enforcement or U.S. government where more things can be done?

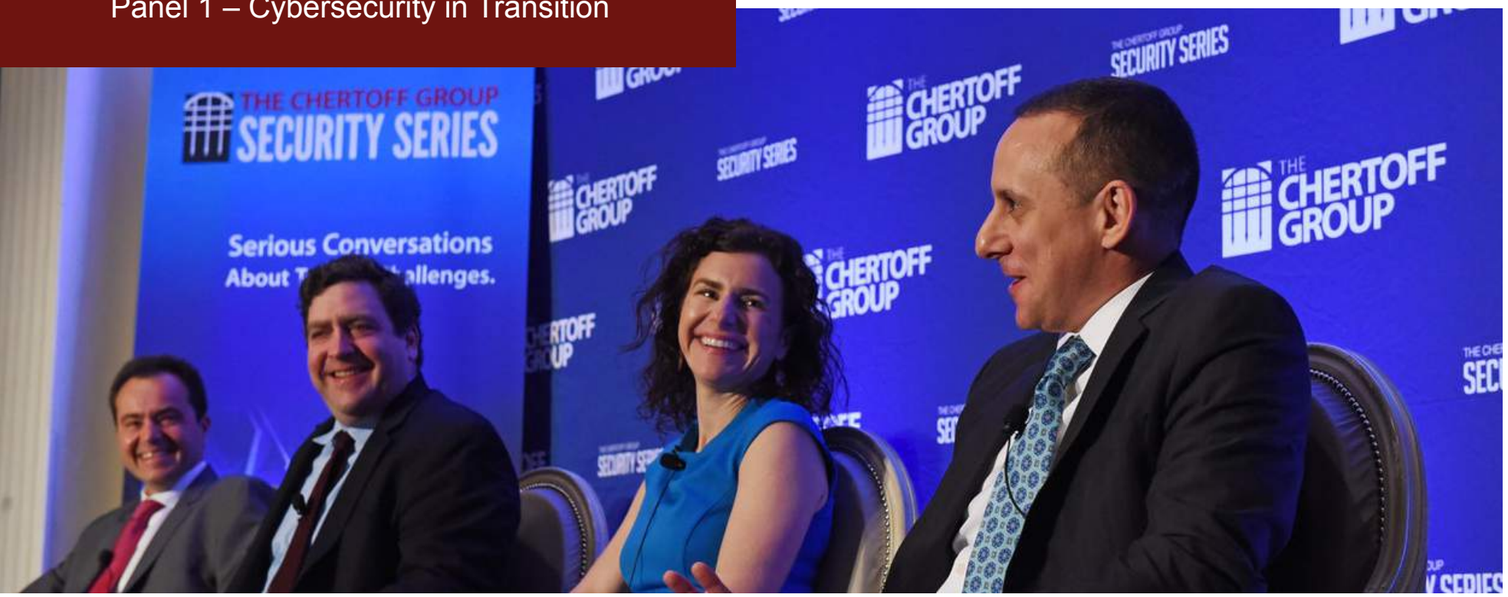
Chertoff: One of the areas of tension that we've seen a little bit over the last couple years between the tech community and the government is on the issue of the tech community now feeling, in the wake of Edward Snowden, that they have to demonstrate not only domestically but internationally that they're not really tools of the U.S. government. So you get a greater emphasis on tech companies saying to the government, 'look we will give you whatever we can give you—information in our possession—but it's got to comply with the law. You've got to show us you have the appropriate legal authority to get this information.' Sometimes that frustrates people in government because they feel the process of getting that authority is cumbersome or unwieldy and they'd really like to just get something on an informal basis. But again on the issue of trust, and particularly on the issue of our global position in the world economically, we need to be able to show the world that we are maintaining a system of law that reasonably protects privacy but of course also allows the government to get what it appropriately should get to protect us. That means we've got to take a look at some of our legal rules about getting information. Traditionally, that kind of cross-border request for information has not been very efficient. We see a lot of unnecessary conflict and one of the things this new administration can do with Congress is come up with a comprehensive set of rules that we can negotiate with some of our overseas partners that creates a streamlined, efficient, and mutually respectable way to get information that is required by law without stepping on someone's toes in terms of their sovereignty. There's a rise in nationalism now in our country, but also in other parts of the world. So they're going to want respect for their national boundaries and we want it for ours and in order to make sure we all don't wind up getting hurt, we need to come up with a common set of standards on these things. If you can do that, we can be quite efficient in providing information when it's necessary. That's an area where I think we can get some forward progress in the next year.

Montgomery: Do you see more education and conversations taking place at the C-suite level when it comes to the security and health of their networks?

Chertoff: People know they ought to be concerned, but they're not quite sure what to do. First, you've got to level set expectations. If anybody goes in and says, 'we want to be immune from hacking,' that's like saying, 'doctor I never want to get sick my whole life.' It isn't going to happen. You're going to get hacked. It's about how you configure your defenses so that you can minimize the damage, detect the problem quickly, and remediate it. Second, it's not just about budget, it's about governance. Many of the fundamental issues of cybersecurity involve making policy decisions. There's a set of deliberate decisions that will affect the degree of vulnerability you have as an institution. And that's not something that the technical guys can decide. Because when the business guys are complaining, the IT guys aren't going to answer that and the CISO isn't going to answer that. That's going to go up to the senior level of management, which is why management needs to understand what are their most strategic assets they need to protect. How does that interface with their business model and particularly on the issue of mobility and data, how do you want to make those tradeoffs? Sometimes it may even be a question about what business you want to go into Do you want to get into this line of business, or does it expose you to too many different things? And those are ultimately fundamental policy and business decisions. What is your core set of business interests? What are the things you're most worried about? And then what are the kinds of decisions you need to make to reconcile those interests and make sure you maximize efficiency and security without compromising fundamental business practices. And that's why this is not a technical problem, although there's a technical aspect to the solution. It's a governance and policy problem.

> "We really need to get to the point where we really view security and privacy as two sides of the same coin and very much interrelated."
>
> – Michael Chertoff

Panel 1 – Cybersecurity in Transition



Summary:

With a historic election cycle in the rearview, many are wondering what lies ahead for the future of cybersecurity? What will a cybersecurity strategy look like in the next administration and what are the key issues that need to be addressed? The Chertoff Group gathered influential experts to discuss potential impacts and explore possible actions for the incoming administration.

Panelists:

Frank J. Cilluffo, Associate Vice President & Director, Center for Cyber and Homeland Security, George Washington University

Kiersten E. Todt, Executive Director, Commission on Enhancing National Cybersecurity

David Perera, Assistant Vice President for Government and Policy, Internet Security Alliance

Moderator: Jason Kaufman, President, The Chertoff Group

Kaufman: How would you help the new administration to understand cyber?

Perera: We are seeing a failure of the private sector to grapple with the issues of cybersecurity just according to fundamental market forces. Cybersecurity is an economic security issue and it's a national security issue. This is exactly the type of wicked problem that the federal government exists to assist with. There are a number of levers that the federal government can pull to try to influence the private sector; regulation is one of them. We believe that regulation has a demonstrated track record of being counterproductive when it comes to cybersecurity. Cybersecurity is dynamic, it's changing, it's resistant to a regulatory approach. Therefore, the lever the federal government can pull is one of public private partnership that also includes incentives. We do believe that there is a role for targeted tax breaks. However, it's a mistake to equate incentives exclusively with monetary incentives. There are things like regulatory relief, liability relief, and other things the government can do to encourage the private sector in order to do cybersecurity at a level that currently is not commercially sustainable. And that's the big thing about cybersecurity. Because it's about national security, because it's about economic security, there is a gap between what the private sector is currently doing i.e. economically sustainable levels of cybersecurity and the kind of cybersecurity that we all know that we need. Filling that gap is the role of a public private partnership. It's the role of incentives."

Kaufman: Let's explore the question around the Democratic National Committee breach. We have a president-elect who will be tested early in the administration in the area of cyber. How should the new administration respond?"

Todt: I think one of the things that we've learned is that there is no big event. Every event continues to evolve and everything is large. So to think that there's going to be a defining event for this administration or the first one—they're all happening right now. It's all out there. And I would argue that the biggest gap right now is really how the public and the private sector are working together. We do need to be collaborating and working together. What are the resources of the private sector that are valuable before an event? What are the resources of the government before an event? We have not created the effective mechanisms to truly access all those capabilities. So whatever the

Panel 1 – Cybersecurity in Transition

strategy is, it needs to be specific and it has to create mechanisms not just in incident response. We need to be looking before the event, particularly when it comes to cyber. And whatever that structure is, it has to be agile. Resilience is really the key here. We're not going to defend against everything, we're not going to prevent everything. But we have to create the agile and flexible infrastructure that creates the most resilient cyber infrastructure so that we kill the low hanging fruit and prevent what can be prevented, but we're always in a place to respond to and contain the detriment of whatever events are coming down the pike.

Kaufman: Could you talk about the NIST framework? What the administration has gotten right and what we should do going forward?

Cilluffo: "The NIST framework is great, but it's a plan-to-plan document when you really get down to it. I almost feel like we have a 'plandemic' of plans. There's a lot of activity. It's figuring out what really matters, figuring out what your outcomes and objectives are and then zeroing in on some of those activities. When it comes to small and medium sized businesses… they are the entities that don't know exactly how to plug in. When you think of the financial services sector in particular, small and regional banks are not going to spend the $600M the big banks are spending a year on cybersecurity. It's preposterous; they can't. But maybe that's where some of the other providers can actually integrate cybersecurity as a cost of doing business and as long as it's within a reasonable amount of money it would be somewhat easier to be able to offset some of that risk where you have teams that are 100% devoted and focused on some of this. At the end of the day, there has been a lot of good activity. The question is: are we ready to implement and execute and actually start moving on some of this? It's not just a resource issue. That's part of it of course. At the end of the day, I'm not sure we've clearly articulated what success looks like."

Kaufman: What role do you think the federal CISO will play?

Cilluffo: "I think it's wrong to pin the tail on one particular entity and give them full responsibility because ultimately the vast majority of breaches are due to [people]—you've got the insider threat, you've got well-intended but people clicking on links. I don't think you can put all that authority in one individual, but I think it is an important step. We're never going to regulate our way out of this problem, nor should we. Technology is changing so rapidly; even if you wanted to go in with that approach, you're going to be years out of date by the time anything gets done in Washington. But I would argue that when we talk public-private partnership, if the government isn't in a position to be able to respond to all these sorts of threats, the last thing they should do is provide obstacles to the private sector and penalize entities that are trying to do the right thing. Where we are today is the equivalent of – if your house gets broken into and your office gets broken into and your building gets broken into, you're calling the locksmith. That's the way we're treating cyber. So we're not going to get through this or over the hurdles if we're just building higher walls protected by wider moats and locked with stronger locks. That's just doomed for failure. It's very reactive. So we've got to start thinking about actions that can be taken where the private sector can utilize some of their capabilities and quite honestly they've got more ingenuity and more entrepreneurial ideas than any government would have."

Kaufman: Can you provide any insights into the upcoming Commission on Enhancing National Cybersecurity report?

Todt: If we're truly going to change this culture of security, we have to be addressing it across the board. Education is really important. Security should be seen as a differentiator. Right now, as a consuming culture, when we look at products, we're not looking to see what the security features are. We don't care. We're looking at the color, we're looking at the apps, we're looking at the design. Security needs to become a differentiator and we need to create the incentives to make that the case. That is part of changing that culture. So we hope in this commission report that we will be creating these actionable solutions for the next administration that can be acted upon quickly, but then similarly we're also looking at how to change the culture in the private sector, both for vendors and the consumer so that we are creating and securing a digital economy for today but most importantly 3, 5 and 10 years into the future.

> "Resilience is really the key here. We're not going to defend against everything, we're not going to prevent everything. But we have to create the agile and flexible infrastructure that creates the most resilient cyber infrastructure so that we kill the low hanging fruit and prevent what can be prevented, but we're always in a place to respond to and contain the detriment of whatever events are coming down the pike."
>
> – Kiersten Todt

Panel 2 – Improving Identity & Trust Online

Summary:

Today's digital environment requires individuals to be able to access data networks from multiple devices and geographic locations in real time. How do we authenticate identities to ensure a more secure environment while creating a simple yet trusted experience for all users? Jeremy Grant moderates this discussion with a panel of experts representing government and private sector organizations and where they focus when it comes to the intersection of identity and technology.

Panelists:

Douglas Glair, Manager, Digital Identity Services, USPS

Katie Crepps, Vice President, Capital One

Darran Rolls, Chief Technology Officer, SailPoint

Craig Shank, Vice President for Corporate, External and Legal Affairs, Microsoft

Moderator: Jeremy Grant, Managing Director, The Chertoff Group

Grant: As you look across state of market, both challenges and opportunities, are you excited or worried? Why?

Shank: I am excited about the amount of innovation that I'm seeing going into identity at the device level, in the cloud, and across the ecosystem. I'm excited about another thing here that I think may be relevant as we talk about new administration conversations. It's easy for us here in the US to center on all of the attacks that we are feeling. At the same time, the US leads in this space. U.S. companies, U.S. industry, I don't just mean tech industry. There is a real opportunity for us to lead across the world. Why do we feel the attacks in the US? This is where the money is. We get attacked because this is where it's easiest to find the money, not because it's where it's easiest to attack. I feel a lot of optimism about the US and the opportunity to lead in securing U.S. assets directly, but also to lead in advancing U.S. business around the world. What am I afraid of? I am afraid of a couple of different things. Inertia – inertial is really tough on us all. And there's complexity across the ecosystem that we have to navigate our way through and I think we could use some government help navigating our way through. And there's complexity in the values ecosystem around the world as you think about principles around privacy, anonymity paired with security. These take some real working through to solve for.

Grant: What's driving your approach towards building PIV-grade security into solutions?

Crepps: I think that we have to be really sensitive to the fact for private industry, especially for things like small business, that the burden doesn't outweigh the value. You can put in all sorts of complex infrastructures but if they have a heavy cost side to them, who are you expecting to use this? This is the Fortune 100 companies, you're not looking at the mom and pop shops or small doctors' offices. I think from a technology perspective we've come to a place that you can pass credentials underneath the covers if you will. So now all of a sudden we can create a frictionless experience for the consumer. The question that comes to mind for me is not the capability to do it—it is how do you promote the uptake? Unless you can find that sweet spot that

Panel 2 – Improving Identity & Trust Online

says the consumer has to show up there anyways? Consumers are happy to hand over their credentials in some circumstances, which is a huge fear of mine. I think there's a better way to do that so you can actually secure third parties in a way that makes sense and gives the consumer control. But I still come back to that first question, which is how do you get a consumer to want to play in that space and use the frameworks that you've outlined and how do you get private industry and government to all work together collaboratively to use the same sort of schema so it's easier for the consumer.

Grant: What should happen next? Looking ahead to the next four years, what would you prioritize?

Rolls: The change in administration is almost irrelevant to the threats and the vulnerabilities that are before us. The problems haven't changed a single bit. The weaknesses that are in the infrastructure are still there and the challenges are the same. I would hope that many of the things that we've seen will continue: a focus on some of the basic principles. The rather sobering fact is today, basic principles of security are not in place in most agencies, in most companies, and in most households. It's basic principles of administration that we can't get lost in. I think some of the things that we've done through CDM are very important. Let's focus on where the highest privilege lies. These principles stay the same, so stay the course and listen to the smart people, and keep funding."

Shank: Standards really do matter. I would encourage continued forward looking at the standards that are necessary for that ecosystem. There's additional work on identity, there's work on secure information sharing, there's work on conformance that needs to be done. I would also urge the next iteration of the kind of projects that NSTIC undertook—I think that would help a lot to drive the private sector. Jumping out of identity and into cybersecurity– the US has a chance to lead for the benefit of our security and for the benefit of U.S. businesses of all types. Things like the cybersecurity framework— the more we can develop those standards and they can become global, the better off we are as nation from a security perspective and the better off we are as a nation from an industry or business perspective."

> "Standards really do matter. The more we can develop those standards and they can become global, the better off we are as nation from a security perspective and the better off we are as a nation from an industry or business perspective."
>
> – Craig Shank

Grant: How do your companies tackle privacy when you're building identity solutions? Do we have the right tools today to actually architect privacy so that consumers are willing to trust these new solutions?

Glair: I think when you look at privacy, it ties in. It's privacy, at the same time as trust and value. The individuals that are using all the companies' capabilities—they're looking and they're making those tradeoffs and decisions, when connecting and signing up for something brand new from a startup, they're seeing enough value there to say, 'I'm willing to give that data because I want that value,' and the moment that value goes away, they leave. So as an ecosystem, we're constantly balancing those decisions with the large support of the ecosystem driving towards, 'we need to do it in a more trustworthy manner to protect our brands and protect our customers.' All those things constantly are in the discussion as to how do you bring more value to the consumer but protect them because you want to retain them as a customer. We still haven't cracked that nut and one of the topics we haven't talked about here that continues to be out there is integrating companies together and the final liability decisions. Unfortunately, something we're all struggling with and figuring out is how do you handle those handoffs, how do you trust one another, and making sure that's there from the liability side.

Panel 3 – Security in the Boardroom

Summary:

In an increasingly digitalized world, every industry is undergoing a technological transformation to remain competitive in the market and connected with consumers. Where does security fit within this transformation and how can corporate leaders use it as a market distinguisher to further growth and business advantage? The Chertoff Group's Adam Isles explores the evolution of cybersecurity at the c-suite level with those responsible for security in their own organizations and how senior executives are balancing security risk and business decisions.

Panelists:

Anthony Grieco, Senior Director and Trust Officer, Security and Trust Organization, Cisco

Deb Fitzgerald, Chief Information Officer, Deltek

Joanne Martin, Chief Information Security Officer, Hartman Advisors

Moderator: Adam Isles, Principal, The Chertoff Group

Isles: How is the conversation about cybersecurity in the boardroom evolving?

Fitzgerald: It was seen as something only I had to worry about, but it's now seen as part of managing business risk. Managing business risk in terms of avoiding catastrophe and it's, 'how can we use security to lean into things like taking our products to the cloud?' Customer trust is fundamental for us, especially as a cloud software company. Security is there and consumers get that. So we're not talking about security any longer from a technology perspective. It's being talked about from a business risk perspective as well as an enabler perspective, and that's a shift that's happened in the last couple years."

Isles: To what extent to you see boards starting to challenge management? Is security thought of?

Martin: When you talk to a board about risk, there are three top topics that ought to be on your list to talk about at every board meeting in terms of how you're doing. Culture—It's one of the big pillars of all this. Winning the hearts and minds and making sure that the culture is one where people know what their vested interest is in protecting, and the board needs to make sure that they're driving management in that direction. The second is data—do you know where your most important data is? Are you protecting it to the right degree? There are different security approaches to handling that most important data. Because if you can't protect everything, know where that is and address it. And the third is how quickly can you respond? When something happens, you're going to protect your reputation by responding quickly and appropriately. Because the difference between – especially for small companies, but it's true with big companies too—really damaging or maybe losing your company and coming through it. If you can have that conversation with your board every meeting, then they may have a few other questions along the way, but those are three really big issues that need to be at the board level and where the board can have an impact.

Isles: Once board and senior management are convinced, what are the key implementation risks that come up as you build program? Where do people get tripped up on the road to maturity?

Panel 3 – Security in the Boardroom

Martin: Underneath, the technology changes quickly. What I see, especially with mid-size companies, is they are partway to implementation and then a new shiny toy comes out and they want to pivot to that, and they haven't finished the first thing first. I think it's better to have 'good' than to have great anywhere. Try to stick to a plan, set a strategy, and make sure you have all the hygiene for it in place. Once you're there, then you can go add the shiny toys. But I think that the rapid introduction of new things that are all very exciting is a huge burden on the team and diverts from the focus of just getting it right and good. There are always going to be new threats and you've got to address them, but most of them are still going to be addressable with your current strategy. If you have to add something, know why you're doing it. To me, that's a big risk; never completing anything because there are new things happening, and there are always going to be new things happening.

Grieco: I think that basic notion of understanding what you are going to put as your bedrock of your strategy from a security perspective is important. And it goes back to not necessarily starting at the technology piece, but the people, the processes, and the policies to really underpin something that is solid. It is easy to go to a security conference and get distracted by the latest and greatest widget. Think about the fundamentals of that strategy and use that to really guide where you're going to go and where you have gaps. To me it is one of the biggest challenges because people talk about it in the context of we're going to spend, but the problem is once you spend and are ineffective or not appropriately making progress, you lose faith. You lose faith of your management, you lose faith of the people who have counted on you, and you actually put yourself in a much worse position. That foundational strategy is important to guide you through that process.

Isles: You're dependent on critical third party partners. What about third party risk? How is the approach for third party risk changing?

> "Understanding what you are going to put as your bedrock of your strategy from a security perspective is important. And it goes back to not necessarily starting at the technology piece, but the people, the processes, and the policies to really underpin something that is solid."
>
> – Anthony Grieco

Grieco: Understanding what is in your supply chain and the breadth at which it is there is really a first step. In many cases, as you look further and further up the supply chain, you get to the small and medium businesses and it's about how to educate and help them understand the need for things like basic practices from a security perspective, so that the dependencies are met all the way up the chain. Once you understand those fundamentals, it is this notion of ensuring that you're managing those risks but then also using it to enable the business. What we've found is the ability to quickly call out and know that particular suppliers or particular technology providers are great partners in the context of security allows us to go fast in delivering product and solutions and services to market. And so part of the conversation has got to be more than 'I'm a big company I'm going to impose a bunch of requirements upstream and go do all these things' – it's about how does that enable the business both for me and for them to be more agile and go off and tackle the problems. That's where I think we've got to pivot this conversation.

What we're also seeing is very active challenges from customers and frankly encouraging customers to ask questions in these spaces about security practices. 'Do you have a security development lifecycle? Are you practicing these things that you ought to be doing when you're selling me something?' Those are really fundamental elements of helping our customers understand that they have dependencies upstream. I think we have an environment where we have a lot of really smart technology companies and people that are very mature in this conversation, and we've got to realize that there's a very broad ecosystem of people out there who are just getting started in this discussion. I think us as larger entities helping those who are newer to the conversation is really part in parcel to us all being successful.

Panel 4 - Transferring Cyber Risk

Summary:

CISOs, CIOs, and board members need to reduce their exposure to hacks and a robust cyber insurance policy can help enterprises weather the storm more effectively when a data breach or network security failure has occurred. This session explored the state of the cyber insurance market and why it is valuable to have cybersecurity insight in today's complex threat environment. The panel shared its predictions for the future of cyber insurance, including the impact of proliferation around the Internet of Things.

Panelists:

Ben Beeson, Cyber Risk Practice Leader, Lockton Companies LLC

Christopher Liu, Head of Cyber for the Financial Institutions Group, AIG Insurance

Chris Goettle, Director of Security Solutions and Strategy, LANDESK

Moderator: Greg Hill, Principal, The Chertoff Group

Hill: How is cyber insurance evolving in dealing with a lack of historical data as well as aggregation models to model risk, particularly with the dynamic nature of today's changing threats?

Beeson: It evolved initially through on-site audits, a barrier to sale, and that just wasn't going to fly. And since then it's been more remote and more sort of what you would see traditionally in other areas of insurance – questionnaire based or interviews – and trying to get an understanding of the security culture of a particular company. Increasingly that's not good enough. The risk is becoming too big and you're also seeing, because of the aggregation issue, there's more pressure. Whether it is from market regulators or within insurance companies themselves to come at this and understand it much better. So the modeling point without any actuarial data is a hot topic for that reason right now. And it hasn't been solved. The premium that you are charged for cyber insurance today is a commercial premium; it's what the market tolerates between the buyer and the seller.

I think what you are seeing [something] that's positive [around] technology emerging. Specific tools and technologies to help insurers model risk and actually help brokers, who find themselves caught in the middle of this issue, help clients both quantify and understand the relationship between the size of their risk and what the outcome of the insurance policy is. Increasingly, we're finding that there is a ROI discussion going on: what is my return on investment on what I'm spending on my technology, policies, and procedures? Where do I sit on the level of maturity as an organization on that curve? Am I at a point where it makes sense for me to insure? And if it does, how much should I buy? Or maybe it doesn't and maybe I need to be putting my dollars still more into my controls?

Hill: How do you see underwriting evolving?

Beeson: Some would say the underwriting process is broken because it's too static and the risk is too dynamic to capture on a questionnaire or a phone interview. What is starting to happen, which is good news, is you are starting to see insurers start to partner with cybersecurity firms and technology firms to try to help address that issue. For example, an outside in tool that looks at corporate networks—it doesn't give you the whole answer but it gives you something, it gives you a data point. And it gives you a data point in real time. Saying that an approach that has worked for

Panel 4 - Transferring Cyber Risk

> "The future of cyber insurance underwriting is going to be hand in hand with the future of cybersecurity in the sense that it's going to be a collaborative effort. It's going to be everyone working together, using all of the technology that we have at our disposal, but also leveraging the information sharing aspects."
>
> – Christopher Liu

insuring hurricane or commercial property will work for cyber—that is definitely not how the industry views this. And we are trying and investing in a different way.

Liu: The future of cyber insurance underwriting is going to be hand in hand with the future of cybersecurity in the sense that it's going to be a collaborative effort. It's going to be everyone working together, using all of the technology that we have at our disposal, but also leveraging the information sharing aspects. As an insurance carrier, we write something like 20,000 cyber insurance policies so we see all of the associated breaches with those, aggregating all of that information, building an ecosystem where our insured clients have the benefit of that experience and the benefit of that data and us working with them to better understand their risks. It's easy for us to say – "we talk to technology and security companies and they say 'these are the ten things that every company should be doing'" and that's fine, but understanding how cyber risk presents in a particular business – the people who run that business are going to know better than anyone else. So it's really going to be working together as a community to both do as much prevention as we can, provide as much response and recovery and tools and services as we can, and write policies sustainably so we'll be there to continue to write checks to cover the financial impacts.

Hill: For companies that work with companies [insurers] like yourselves that go through the top ten and actually demonstrably improve their cybersecurity posture, at what point will the carriers via the broker start incenting that behavior with reduced premiums?

Liu: Being the invisible hand of the market and saying well I'm going to charge you 10% more this year because you didn't keep up with your insurance with your security posture—I don't think we're quite at the point yet where we're able to influence on that scale. What I will say is we are doing that already. Your limits, your retention, your premium, and your coverage are all already dictated by your level of security risk and your security posture… We have had a couple of type companies who have gone into the market and haven't been able to procure insurance partly because they weren't overcompensating for their natural industry risk with top of the line controls, but they are getting there. And I think what they're turning to now is innovative insurance products that are going to be more willing to cover those risks [rather] than modifying their behavior to get into traditional cyber insurance policies. But I think we are going to get there. But because we have all of the relationships with forensic investigation firms, privacy counsel, and so on and so forth to deal with incidents when they happen, we're leveraging those relationships and those preferred rates and that expertise on the front end so you buy an insurance policy and it automatically comes with services. So just getting into the insurance market and being a cyber insurance participant is already raising the level of security generally in the industry, although I recognize the frustration that we're not getting there all together.

Beeson: Incentives are brought up a lot. We're not far away from some significant losses, and that's because of IoT, and that's the elephant in the room in many ways, which is something that really has just only raised its head this year in the industry. It's been very PII focused, very PHI focused. Now we get into issues of property damage, bodily injury, business interruption. I think the way to sum that up right now is ambiguity. When I said cyber insurance is a misnomer, that's because of IoT. Because now, this risk and its consequences got much broader than PII liability. It's now actually overlapping with other areas of insurance that you may already buy. And that makes it very complicated right now. It's not getting any easier. We've got issues of aggregation, we've got issues of risk modeling, and now we've got issues of coverage because the risks are broadening and driving additional consequences.

Hill: What do you think buys down risk the most?

Goettle: There's always a balance. There is no 100%. There is no way to fully defend against cyber risks. Just like you can't defend against ever having a car accident. You can't control what other variables are going on. You can't control things nobody's even dreamed up yet. One thing that's always interesting is seeing what the hackers come up with next to exploit our environments. So cyber insurance is absolutely necessary, and I think it is up to each company to decide what is the right balance for them? Putting more dollars towards that versus other things. The one thing I would say is make sure that you are continuing to mature your security practices in general. Ger to the point where security is no longer a process or a security control, it becomes a discipline. That's the most important thing to make sure that you're not wasting your insurance dollars. Not whether or not you should have it—you should have it. At some point you can and will potentially be breached. But, don't neglect making sure that you are making security a discipline within your organization." –Chris G

Spotlight Session: David Bray is the Chief Information Officer for the Federal Communications Commission

Fostering Cyber Resiliency as the IOE Exponetially Expands

David Bray is the Chief Information Officer for the Federal Communications Commission and an Eisenhower Fellow to Taiwan and Australia. He has first-hand experience with regional strategies focused on the Internet of Everything (IoE). During his spotlight session, Bray emphasized the urgency with which the U.S. government must encourage both public service and public-private partnerships to foster cyber resiliency as the IoE exponentially expands.

Our world is rapidly changing: there are more than one billion web servers today, and the last 150 million came online in the last two years. The problems before us are even further complicated as more and more IoT devices are combined with complex legacy infrastructures, machine learning, and human actors. Last year, there were about 14 billion network devices for the 7.3 billion humans on earth. By 2022, there may be 75 billion devices for only 8 billion people. This exponential expansion is breaking the paradigms we know about cybersecurity.

This type of expanding change will strain both the public and private sector, with implications spanning privacy, the economy, and security. The IoE is constantly producing personal data, both intentional and unintentional. We will fail to capitalize on significant opportunities because we are literally drowning in our own data. Similarly, current cybersecurity practices will fail to scale and keep pace with this proliferation of data.

Like infectious diseases, cyber threats traverse borders and affect entire communities. Bray argues we must take a new approach—one akin to public health—to foster cyber resiliency. Bray suggests the U.S. government and industry come together to form a public-private partnership: a non-profit “cyber CDC.” Today, there is no way to gauge the health of the Internet, and the “cyber CDC” could fill this void. A “cyber CDC” could serve as a hub of innovation and research. “Change Agents”—people willing to step outside the status quo—could analyze IoE abnormalities leveraging artificial intelligence and regularly share a “cyber epidemiology” including cyber signs, symptoms, and behaviors of IoE devices. As the IoE rapidly expands and today’s cyber practices break, a “cyber CDC” could provide the space to explore new methods to bolster privacy and cyber resiliency.

> “We should consider creating a public-private partnership that provides a space for cyber Change Agents to research and explore approaching cybersecurity differently – focusing instead on cyber resiliency and an approach more akin to “cyber public health”
>
> – David Bray

"The future of cyber insurance underwriting is going to be hand in hand with the future of cybersecurity in the sense that it's going to be a collaborative effort. It's going to be everyone working together, using all of the technology that we have at our disposal, but also leveraging the information sharing aspects."

– Christopher Liu

"Resilience is really the key here. We're not going to defend against everything, we're not going to prevent everything. But we have to create the agile and flexible infrastructure that creates the most resilient cyber infrastructure so that we kill the low hanging fruit and prevent what can be prevented, but we're always in a place to respond to and contain the detriment of whatever events are coming down the pike."

– Kiersten Todt

"We really need to get to the point where we really view security and privacy as two sides of the same coin and very much interrelated."

– Michael Chertoff

"We should consider creating a public-private partnership that provides a space for cyber Change Agents to research and explore approaching cybersecurity differently – focusing instead on cyber resiliency and an approach more akin to "cyber public health"

– David Bray

"Understanding what you are going to put as your bedrock of your strategy from a security perspective is important. And it goes back to not necessarily starting at the technology piece, but the people, the processes, and the policies to really underpin something that is solid."

– Anthony Grieco

"Standards really do matter. The more we can develop those standards and they can become global, the better off we are as nation from a security perspective and the better off we are as a nation from an industry or business perspective."

– Craig Shank

HOUSTON
1800 West Loop South
Suite 1790
Houston, TX 77027
713-865-2855

MENLO PARK
68 Willow Road
Menlo Park, CA 94025
650-294-4821

NEW YORK
183 Madison Avenue,
Suite 903,
New York, NY 10016
646-289-6840

WASHINGTON, DC
1399 New York Ave, NW
Suite 900
Washington, DC 20005
202-552-5280

www.chertoffgroup.com