FEATS OF STRENGTH

A BUSINESS-FOCUSED INFORMATION SECURITY MAGAZINE

2017 TRENDS

March 2017

CISO PROFILES & 2017 TRENDS

Cyber Insurance
Decentralization of Information Security
Security Product Clutter
Government & Cyber Security

K logix

Earning the right to be confident in information security

WWW.KLOGIXSECURITY.COM 888.731.2314

FEATS OF STRENGTH

MARCH 2017

PROFILES IN CONFIDENCE

FEATURES

LETTER FROM

KEVIN WEST

CEO

THE 3 BILLION DOLLAR NOISE MACHINE

After yet another article listing the Top 500 security products popped up in the news, I realized I had hit my tipping point. As security practitioners, we want to focus on strategic, business enabling objectives, yet can sometimes be clouded with the overly saturated amount of data being thrown in our direction. As CEO of a security organization, my problem is the same problem many CISOs face, with an enormous influx of similar messaging and clutter in the market.

According to CB Insights, venture capitalists and investors poured $3 billion dollars into more than 300 deals in the cyber security industry in 2016 alone. That's a lot of powerful organizations betting on the growth of the cyber security market.

What does this mean for CISOs?

Well, it means there are plenty of innovative products to check out, but also a lot of noise and distractions. These well-funded security startups have CISOs in their target. With these investment dollars, startups are attempting to dictate security conversations and frame challenges in terms of their own solutions.

It takes a lot of discipline from a CISO not to be distracted by all the bells and whistles on display. The vendor onslaught combines with daily, sometimes hourly, news headlines about data breaches. It is no wonder that CISOs sometimes feel like they are trying to get their work done in a packed football stadium. It can be hard for even the most mature CISOs to concentrate on their strategic priorities.

In this issue of Feats of Strength, we profile many CISOs who are veterans of the industry. While they report an increased number of startups on the scene, they have suggestions for how other CISOs can manage it all. In his profile (pages 16-17) Ed Ferrara, CISO at CSL Behring says, "The VCs see this [the threat landscape] as a growth industry." He

continues, “At the end of the day the customer needs to do a lot of due diligence. Speaking as a former analyst, I can say that due diligence means doing more than just reading the analyst report and buying the recommended technology. Consider how the technology fits within your business model.”

In his profile (pages 6-7), Michael Coates, the CISO of Twitter suggests making sure any new security technology investments make sense for your organization. Does it solve a real and pertinent challenge, and can it run without a big time and management investment from your team. Coates says, “Security needs to be scalable, fast and effective at addressing real problems. Security technologies that create a lot more work for already overburdened security teams are not helpful. If I can trust a security solution to do its job then I can focus my team’s efforts on one of the many other issues we face.”

We cannot ignore that some of the noise distracting CISOs and their teams comes from within the existing security infrastructure. Many companies already run 20 to 30 information security products, which produce countless numbers of notifications and alerts. In an article on effectively leveraging and managing technology investments, Don Cook, Director of Program Management for K logix suggests that every information security solution, whether already installed or yet to be purchased, should be evaluated based on operational impact, risk mitigation and financial impact to the business. “If you cannot tie a product back to your vision and security strategy, then it is not a sound investment,” says Cook.

Dr. David Reis is the CIO at Lahey Hospital and Medical Center. Formerly a CISO, Dr. Reis asks himself two questions every day. These questions help him stay focused on business priorities.

He asks:

“Have I made it easier for my organization to successfully implement digital strategy?”

“Did I communicate security’s impact on business effectively, and in our specific business language, to other executives.”

Dr. Reis’ two questions should guide CISOs actions this year. It is impossible not to acknowledge the noise, but CISOs have a job to do and that is to enable a secure environment for their business. CISOs that create a comprehensive security plan and routinely cross check financial and time investments against their plan will have the most success blocking out the noise and delivering on their promise to the business.

THE CYBER SECURITY INVESTMENT CRAZE

Most funded security products in 2016:

- Mobile security
- Vulnerability & risk management
- Network security
- SCADA security
- Incident response

Back to business? The market for startups is slowing down (slightly)

2015 saw $3.75B invested across 336 deals, compared to 300 deals and $3 billion in 2016.

KEVIN WEST is the founder and CEO of K logix, a leading information security company based in Brookline, MA. K logix helps create confident information security programs that align with business objectives.

SECURITY PRODUCT OVERLOAD?

A look at how K logix understands and measures how technology investments fit in security programs.

Contributor: Don Cook, Director of Program Management

The Security Product Overload Challenge

The security product overload is an enormous challenge facing many CISOs and security leaders. Don Cook, Director of Program Management for K logix says, "New CISOs, even experienced CISOs, come in to a new organization and they are overwhelmed by the multitude of existing technology investments. Is it solving the problem it was originally purchased to solve? Do I have clear visibility to effectively utilize the investments? How do I ensure they are aligned to identified risks?"

Answering these questions may be a challenge for many CISOs. To address this, K logix has developed a **Technology Gap Assessment** to help CISOs understand and measure how technology investments fit within their information security programs.

TECHNOLOGY GAP ASSESSMENT:
Clear visibility to effectively utilize technology investments and ensure they align to identified risks.

K logix's Technology Gap Assessment Process

Cook says to understand the effectiveness of a specific investment, technology must be evaluated via three lenses:

1. Operational Impact – Is the product fully implemented, supported, and being used to its maximum value?

2. Risk Mitigation – CISOs need to understand how a technology investment helps reduce risk. One way is to reference the Critical Security Controls Top 20. CISOs need to identify security domains that are over or under-invested in the environment as measured against strategic security goals.

3. Financial Cost – The total cost of operating, and supporting a security solution, including staff required to manage the solution must be weighed against its impact on the overall strategy. A CISO should have the ability to look into the future and anticipate where investments in technology may need to shift in order to align with strategic goals.

K logix's Technology Gap Assessment Outcome

Through interviews and information gathering workshops, K logix explores the technical security controls and business impact to determine the current operational posture of each solution. This service answers these critical questions:

1. Are my existing security solutions implemented effectively and realizing maximum value?

2. Are these investments achieving their desired goals?

3. Are these investments keeping pace with the evolving organization?

4. How well are my security investments operationalized?

5. How effective are my people at managing these security investments (including documenting process)?

6. How do these security solutions align to a framework that can be leveraged to make strategic risk-based decisions?

7. In what areas am I underinvested, and where am I overinvested?

8. Is there an opportunity to shift funding to risk areas that need more attention?

Technology Gap Assessment in Action

Recently, a CISO undertook a K logix Technology Gap Assessment to understand and analyze the multitude of security technology solutions in his environment. "The assessment provided a clear picture of the technology investments in my program including their maturity, documentation, deployment status, alignment with SANS CSC, and effectiveness. I was able to identify problem areas to be addressed, and justify my direction and shift in funds, to meet our strategic priorities."

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

MICHAEL COATES
CISO, TWITTER

HEADQUARTERS: San Francisco, CA

EMPLOYEES: 3,600

ANNUAL REVENUE: $2.5 Billion

Many CISOs begin their careers as technologists, yet it is the combination of technology and business strategy that ultimately drives their interest in information security. Such was the case for Michael Coates, the CISO of Twitter. Coates says, “The exciting thing about information security is that it is not just a technical challenge. The truth is, the best technical security answer could potentially drive a business into the ground. The challenge of finding security solutions that work strategically for the business is exciting.”

Coates says he was drawn to the CISO role at Twitter because of the organization’s greater role within the world. “Many organizations need security to be effective, such as banks and government agencies. At Twitter, security is absolutely vital for a safe user experience. Twitter is a platform that allows people to speak truth to power all over the world. For that reason, we need to ensure a safe and secure experience for each and every user.”

As a business, Twitter is only successful if users trust the company’s security efforts. This reality motivates Coates and his team everyday. It also elevates security within the organization, as a basic core of the platform’s mission.

> “The key is to explain the risk as it relates to the business and get prioritization and buy-in from leaders across the whole company”

“Twitter has a massive amount of public information. We enable people to share incredibly mundane and also incredibly important information. With that we maintain a large amount of private information that our users give to us, such as contact information and their location. We are only in the position we are in because we maintain their trust that we can protect their private data. Our role as a security organization is to protect that data while maintaining the speed and real-time design aspects that are key to the user experience.”

In the two years Coates has been CISO at Twitter, he and his

team have elevated the role of security. It now holds senior leadership visibility and support. The company continues to win awards for its security efforts, and is regularly named to the top spot of the Online Trust Alliance Honor Roll.

MAKING SECURITY A COMPANY-WIDE POLICY

One of the most important aspects of Twitter's award-winning security program is senior leadership involvement and company-wide awareness.

Coates says, "Awareness of security is an important topic because security can be a funny thing. If there is no problem today, others might say, 'well what has the security team been working on?' But if there is a security issue, then still others will say 'well what has the security team been doing?' That is why it is always important to be communicating about security efforts and programs."

Coates suggests finding ways to measure ongoing programs and take a quantitative look at security metrics and business risks. Coates believes it is important to bring in other business leaders outside of the security controls organization to understand and measure security. At Twitter, the Security Committee, which is comprised of key business leaders and heads of organizations, takes a quarterly look at overall security efforts as they relate to business performance.

This approach has enabled the team at Twitter to tackle longstanding risks that were previously deemed too daunting. "The key is to explain the risk as it relates to the business and get prioritization and buy-in from leaders across the whole company." Coates recommends starting with a problem that has a clear path to success to build a reputation and show what can be achieved with cross-organization efforts.

HIGH RETENTION RATES IN A COMPETITIVE MARKET

"One reason I wanted to be a leader was I felt I could accomplish more by aligning a team on an objective," comments Coates. Based on his successes with retention and job satisfaction, it seems that the approach is working well for Coates.

Without a doubt, one of the biggest factors in Coates' success at Twitter, and Mozilla before that, is his ability to retain his team of security engineers in a hyper competitive market. "When given a choice of where to work, people stay with me. That makes me very excited. I'm very proud of being able to hire and build security organizations where people enjoy what they do and want to stay here." Coates believes some of the success comes from growing his team internally, rather than having to fight for security talent in the market.

"We have found success in growing our own security engineers. Creativity is an important quality for a security team member, and certain technical skills are needed, but security knowledge can be taught. We take employees with base foundational skills from another team and then teach them about security. What we found is enterprise or network security engineers can come from network or IT backgrounds and web developers can make excellent web and application security engineers. These people have deep knowledge of how the organization runs and how systems work. They know how people do their jobs and how security measures will impact the job. This knowledge is extremely valuable when building security programs that can be effective and not constraining for the organization."

SECURITY START-UP SPACE

The security start-up space is hot and growing. In fact there has been a 300% increase in venture capital investment in security vendors. It can be tough for CISOs to navigate the crowded and noisy market.

Coates believes many security starts-ups are focused on the big news issues, whereas enterprise organizations still have to worry about more traditional security concerns. He says, "I welcome continued investment and experimentation in the security industry. We need a lot of failures to find success. Many start ups are going after challenging areas and it is just not practical. Why worry about a burglar parachuting in when you left the porch door unlocked? Security needs to be scalable, fast and effective at addressing real problems. Security technologies that create a lot more work for already over burdened security teams are not helpful. If I can trust a security solution to do its job then I can focus my team's efforts on one of the many other issues we face."

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

TIM MCKNIGHT
CISO, THOMSON REUTERS

HEADQUARTERS: Toronto with offices globally

EMPLOYEES: 45,000

ANNUAL REVENUE: $11.2 Billion

"Someone called me the CISOs' CISO, just because I have been at it for so long," says Tim McKnight, CISO at Thomson Reuters. In an emerging field, where as many as 80 percent of CISOs are in the position for the first time, McKnight stands out as a veteran with a multitude of best practices to pass along. He says, "I've been a CISO for 16 years and before that I was a special agent with the Federal Bureau of Investigation." McKnight even helped create the first high tech crime unit, the precursor to cyber security, for the FBI in Philadelphia.

In his career, McKnight has seen the role of the CISO progress dramatically, from a back office position to a critical role in the company, helping to map strategy and align security with business goals. He says, "In the early days, the CISO was more of a network security person in middle management. But now we have progressed to have a seat at the [executive] table, and an important voice with the CEO and the Board. It feels like the progression happened over night, but that's not true."

After nearly a decade in the FBI, McKnight took on CISO positions at Northrup Grumman, Fidelity Investments and GE. He has been the CISO at Thomson Reuters for a little more than three months.

"What drew me to the position at Thomson Reuters is the growth trajectory, both for the company, and for myself professionally. The team at Thomson Reuters recognizes that security is on the forefront of enabling growth. Our customers include big banks, accounting and law firms. These are institutions that honor trust and demand integrity. At Thomson Reuters, trust is highly valued and information security is critical for our customer. For me, there is an opportunity to raise the bar and make security part of the value proposition to our clients."

A PROVEN PROCESS FOR THE FIRST 90 DAYS

McKnight has a standard process he deploys when approaching any new CISO role, and in his first 90 days at Thomson Reuters he's worked through that methodology. "It's a traditional approach – people, process, technology, in that order," says McKnight. "In the first 90 days we put a focus on the leadership team and the skillset of our overall team. What are the gaps we have in our skill set? What are our needs for the future, such as the cloud? We did a market analysis of the competition. What do we need to do to attract, retain and develop talent? All of this is a catalyst to move our security team forward."

> The greatest business advice I ever received was from a 92-year-old founding partner at a Financial Services firm. He said to me, 'Tim, you can never know the influence or authority of a person based on where they are in the org chart. There are folks in every company who drive the company. Seek out those folks, they are not just the executives in your line of sight.

He continues, "Then we look at our processes and answer a series of questions. How do we prioritize risk? Are our processes mature and value add? Do these processes mitigate risk to the company? What is the role of the team in risk management? What do our lines of defense look like?

"Lastly we look at the technology portfolio. Where do we have duplication? Does our technology align with our future strategy? Are we getting the greatest use out of our investments? Once those questions are all answered, then we go into planning for the year."

ADVICE AND CAUTIONS FOR NEW CISOS

While this is not McKnight's first transition into the CISO role, he is still cognizant of the challenges new CISO's face. He says there are three especially difficult aspects to taking on the CISO role for the first time:

1. LETTING GO

"So many CISOs come into the role from a technology or network backgrounds where we are hands on technically. It can be hard to let go of the technical functions. But, the CISO position requires management skills, communication skills and business strategy acumen, so it's a real shift in focus for a lot of first time executives."

2. LEARN TO TRUST YOUR TEAM

"When you move from a tactical day-to-day mindset to a strategic view you have to trust your team to keep the daily efforts moving. A CISO's role is about framing challenges, identifying resources and funds, developing strategy and communicating with the larger organization. "

3. COMMUNICATION AND TRANSLATION

"You can't speak like a technologist anymore. CISOs need to translate cybersecurity issues into business risks that CEOs, CFOs, General Counsels and the Board can understand. "

For new CISOs facing these challenges and the daunting work of starting in the role at a new company, McKnight offers this advice, "Identify your key stakeholders across the company, what I call the "super nodes". Those are the people who can torpedo a project without notice or help you become successful."

McKnight continues, "The greatest business advice I ever received was from a 92-year-old founding partner at a Financial Services firm. He said to me, 'Tim, you can never know the influence or authority of a person based on where they are in the org chart. There are folks in every company who drive the company. Seek out those folks, they are not just the executives in your line of sight.'"

McKnight recommends adding those individuals with special influence to an information security counsel or committee so that they are "part of the parade, not sitting in the stands."

The more traditional executives, such as the CIO, CEO, CFO and General Counsel make up McKnight's "Sphere of Influence". These are the people any CISO needs on their side in order to be successful. McKnight recommends approaching them with specific goals in mind. Ask for their support, and request their help on two or three specific initiatives.

THE IMMEDIATE FUTURE OF INFORMATION SECURITY

McKnight says that there is always the next thing to figure out in security, it is not a problem that is ever solved. As a CISO you must embrace change now more than ever before. Organizations are going through significant transformations and CISOs need to be in the driver's seat of this change.

McKnight believes the cloud continues to be a massive trend that requires a large investment from security. His team is constantly reviewing how to better secure the cloud, limit gaps and improve automation related to cloud security. According to McKnight, other big trends for the next year are artificial intelligence and analytics. The Internet of Things will continue to be a large focus as people, cars, homes and life are increasingly connected. Security and privacy efforts will continue to converge, creating new challenges for organizations and their clients.

CYBER INSURANCE

WHAT IS IT?

IS IT WORTH IT?

WHAT ELSE SHOULD IT PROVIDE?

Contributors: Dr. David Reis, CIO, Lahey Health &
James Sheehan, Principal, Integro Group

- As of 2015, cyber insurance was a $2.5 billion dollar industry in the US. It is expected to increase significantly this year and reach as high as $7.5 billion in 2020.
(Cyber Risk Threat and Opportunity Report)

- In 2015, 63% of companies were insured against loss of income due to a data breach.
(Statista)

- More than a quarter of underwriters responded that clients frequently seek higher limits for cyber insurance premiums.
(2016 Survey of Cyber Insurance Market Trends by Advisen)

- In 2016, healthcare organizations were responsible for the most new cyber insurance policies.
(2016 Survey of Cyber Insurance Market Trends by Advisen)

> "The maximum a company can be insured for is about $500 million, but the reality for many companies is that it's tough to even get coverage for $300 million."
>
> - Don Ulsch, a senior managing director at PwC, quote from SC Magazine

Industry leaders and cyber insurance providers weigh in on this emerging, and increasingly important element of any cyber security strategy.

Dr. David Reis, CIO at Lahey Health has been involved in the review and purchase of cyber insurance at several organizations. "Is it necessary? Yes. Is it working? I'm not sure," says Dr. Reis.

Dr. Reis says that cyber insurance is necessary because it is an effective tool to help organizations understand and mitigate risk, and it is useful because it does cover some of the real, hard dollar costs of a breach. He continues, "First, cyber insurance is provocative. It helps CISOs focus business leaders on what needs to be done. Cyber insurance comes with its own set of requirements, or terms, that the organization has to meet in order to be covered. The information we need to give to the insurance provider just to get a quote on cyber Insurance is a good way to give insight to non-IS executives about what we are doing, and what we need to be doing to effectively mitigate risk."

"Second, cyber insurance is necessary because it covers the real cost of a breach. There are real, quantifiable costs to a breach – including costs of notifying customers, replacing systems, and incident response."

The Future of Cyber Insurance

Dr. Reis feels that cyber insurance has a way to go before it is truly effective. "In information security, as an industry, we are struggling to understand the likelihood of a specific breach. This is something I think the cyber insurance industry is, or should be, moving towards. For example, with flood insurance, we know exactly how likely it is that an area will experience flooding. Actuary tables exist to help insurance providers and their clients understand the risk. We need actuary tables for the different types of threats. We need cyber insurance to get to a point where everything can be objectively defined – here is your risk, here is what you are doing to stop it, here is how likely you are to experience a specific breach."

James Sheehan is a Principal with Integro Group, an insurance brokerage, and heads its Cyber Practice. Sheehan notes the cyber insurance market is growing quickly and that organizations are changing their approach to cyber risks. Historically, cyber insurance was purchased as part of an organization's management liability program. As such, the CISO's role was limited to providing information concerning an organization's IT security posture. However, over the past three renewal cycles, Sheehan has seen the CISO become an integral member of the insured's risk management team, with responsibility for providing both updated IT security information and guidance with regard to potential new exposures.

Sheehan agrees with Reis that cyber insurance is a great way to hedge against known risks and the hard costs of a breach or data loss, but he also understands that companies and insurance providers are struggling to appropriately quantify and insure the true cost of a breach – which includes intellectual property theft and damage to the brand.

Still, given its current limitations, Dr. Reis is, in general, a fan of cyber insurance. He says that all CISOs should be considering it. "Ask if we have it, and should we think about it, given our risk profile."

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

MARY ANN DAVIDSON
CSO, ORACLE

HEADQUARTERS: Redwood City, CA

EMPLOYEES: 136,000

ANNUAL REVENUE: $37 Billion

"My goal is a strange one - I want my team to be redundant over time. I want it to be that we get so good at secure engineering that the only thing left for our team to do is routine oversight. We are fundamentally making security a cultural value at Oracle."

- MARY ANN DAVIDSON

Integrity and an unwavering commitment to speak up when there is a problem are the key attributes that earned Mary Ann Davidson the first CSO role at Oracle Corporation.

"When the CIO offered me the position of CSO I was a little surprised. We had several astute IT security professionals in the organization," Davidson comments. She thought others may have been a more obvious fit for the role, as she came from the product management side of the business. Davidson continues, "But our CIO felt that I was the person who would scream when things are not right, and the role requires that. Oracle values when employees speak up. The fact that Oracle demands a level of core integrity to always do what is right, really speaks to the kind of company Oracle is, and why it is a great place to work."

Oracle considers security a core business value. Davidson believes this makes her job as CSO slightly easier than it might be for her peers in other organizations. Since the inception as "Project Oracle", building the first relational database for the CIA, security has been a priority for Oracle. "Now, of course, we have more products and customers across government and all types of industry, but the inherent need for security is still there. Because security is a core value, I have the authority and respect to do what needs to be done to make our products more secure."

THE PRODUCT SECURITY CISO

Due to the nature of the business and importance the company places on

> The Marines have a saying ‘every Marine, a rifleman’; it means every single person can defend the others. In business, every single person should be empowered with security awareness. Oracle is building a culture of security where everyone is focused on it.

security, Davidson has two peers who direct other aspects of the security program within Oracle. While she focuses on assurance, specifically making certain Oracle products have security built in, other security leaders in the company focus on physical security and enterprise security policies.

“My focus is assurance. How do we engineer security into all our products, our cloud services and consulting – everything we sell to customers? If you don’t build security in from the beginning it is less likely to be secure. There is no magic security pixie dust you can sprinkle on the product at the end.”

“My goal is a strange one - I want my team to be redundant over time. I want it to be that we get so good at secure engineering that the only thing left for our team to do is routine oversight. We are fundamentally making security a cultural value at Oracle.”

Davidson makes an engineering analogy to emphasize the importance of building security into every product: “Civil engineers know they have to build buildings to be structurally sound from the start. Security is just like that.”

“Years ago, when I started working in business, the entire world was less IT intensive, so maybe security mattered less. Now, technology is infrastructure – it needs to be structurally sound. We need to ask, how can this be broken, where can it be attacked. This has to be everyone’s approach, whether business people or coders, they have to be thinking about structural integrity and security.”

Davidson uses another analogy to describe the importance that every member of the organization thinks about security. “The Marines have a saying ‘every Marine, a rifleman’; it means every single person can defend the others. In business, every single person should be empowered with security awareness. Oracle is building a culture of security where everyone is focused on it.”

CUSTOMER FACING CISO

Davidson says one thing evolving for her and her team is how much information customers are requiring from the security team. She comments, “Customers are much more interested in how we built the product, and that is a good thing. You want people to ask these questions, and as a result we spend more and more time talking to customers.”

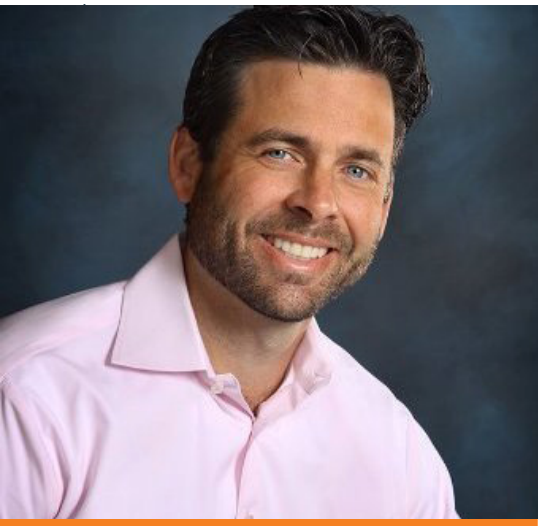
ADVICE FOR NEW CISOS

As Davidson realizes, not every CSO is in a security-aware organization such as Oracle, and some of her peers are struggling to elevate the importance of security within their company. Davidson points out that “responsibility without authority equals frustration.” However, there are specific steps CSOs may take to help prove the business value of security, thereby increasing relevance and authority.

Davidson believes economics plays a large part in making the case for security. “People say security does not pay, but of course it does. Why does it pay to engineer security into the product? First, it’s a brand issue. A secure product has customer confidence. It’s also a cost avoidance. When products have security built in, less money is spent down the line fixing vulnerabilities. If we catch a problem from the beginning, it requires a lot less time and money.”

Q&A WITH ROB GREER

CMO & SVP PRODUCTS, FORESCOUT



> **ForeScout is transforming security through visibility. You cannot protect what you cannot see, and ForeScout's unique approach addresses that need.**

With over two decades of technology industry experience, Rob Greer possesses an expansive perspective and a profound background in cybersecurity. Currently, Greer leads the product and marketing organizations for ForeScout Technologies. His primary mission is to provide the glue that links together the market needs, what to build and how to go to market.

Q: WHAT ARE KEY HIGHLIGHTS IN YOUR CAREER?

I've had a unique career path. The first ten years I worked as an IT security and information technology practitioner, which enabled me to understand how to use technology to solve real business problems. I then successfully built one of the pioneer companies in the managed security services market before transitioning from a technology practitioner who worked with many vendors to actually being a vendor and playing on the other side.

Now that I am at ForeScout, my previous experience across sales, sales engineering, professional services, support, marketing and product management allows me to better partner with our customers and value added partner community as I understand their businesses and the problems they are trying to solve.

Q: WHY DID YOU JOIN FORESCOUT?

One of the reasons I joined ForeScout was the clear passion, experience and commitment of our leadership team. We have a highly engaged Board of Directors, which represents the best of the best in the cybersecurity industry. I realized there was a huge opportunity to be part of a company that offered differentiated and proven technology sold at scale to the largest institutions in the world. With my strong technical pedigree, as well as my sales and marketing background, I had a chance to really make a difference on the team and an impact with our customers and partners.

I also joined because ForeScout is transforming security through visibility. You cannot protect what you cannot see, and ForeScout's unique approach addresses that need. The company is also a unifier of the disparate information security market. We make existing IT and security tools smarter by sharing relevant device context as well as taking actions that most tools are not in a position to execute, such as taking a device off the network.

Q: WHAT IS FORESCOUT DOING IN 2017?

In 2017, ForeScout is defining IoT security. Our strategy, messaging and tactics are focused on helping organizations secure IoT by first gaining visibility and control of devices connecting to their network. Our agentless approach makes this possible at scale. Once ForeScout discovers, classifies and assesses these devices, our technology then makes other IT and security tools smarter by sharing their 'context'. ForeScout is the only player in IoT security that focuses on connecting disparate IT technologies as a full-time business – not a front for selling switches, servers, operating systems and security services.

Q: WHAT CONVERSATIONS DO YOU HAVE WITH CUSTOMERS AND CISOS?

The most common question I hear from customers is, "How many devices do you believe ForeScout will see that I don't already know

CALCULATING BUSINESS VALUE

According to a 2016 IDC Research Study, "IDC believes that one of the key attitudes for organizations to adopt is that of "already breached." This attitude focuses on visibility and detection, with strong remediation capabilities. Instead of perfectly protecting each and every vector, this attitude encourages constant vigilance and the ability to respond quickly, making the organization's security agile enough to meet the rapidly changing business and threat landscape. One solution that addresses this idea of pervasive device visibility and control is ForeScout's security solution."

Source: IDC White Paper; The Business Value of Pervasive Device and Network Visibility and Control with ForeScout. December 2016
For the full report, visit http://resources.forescout.com/idc_businessvalue_bdm_klogix.html

392% five-year ROI

24% more known devices

50% fewer network-related security breaches

about?" CISOs are able to see up to 60 percent more devices than they did prior to deploying ForeScout. This usually drives enough attention to find the necessary budget. Additionally, budget often already exists for endpoint protection, endpoint detection and response and network access control projects prior to ForeScout being evaluated.

I was recently with the CISO of a large UK bank and her biggest challenge was answering the question of 'how secure are we?' I asked her if she knew, in real time, what is connecting to the environment across the entire enterprise. This is key because having a comprehensive view of what devices are connected provides a clearer backdrop to have a conversation with the board. She said she had no idea, but knowing this would provide a sense of confidence in terms of visibility and potential exposures. I discussed with her how transforming security through visibility is a business problem the board wants to understand. You cannot answer the question around whether or not you have security exposure without understanding what's connecting.

Q: WHAT TRENDS DO YOU DISCUSS WITH CUSTOMERS?

Organizations are recognizing that IoT is real in the campus; the days of voice, audio video, physical security systems, HVAC, etc. being whitelisted by IT are over. Organizations have adopted operational technologies (OT) that are now IP-connected – from healthcare, to retail, to power and gas, to manufacturing, and more – and they need to monitor and secure those business-critical devices that in the past were air gapped from other IT services. Organizations are also moving to the cloud across all vectors including data, apps and infrastructure. They are looking for a single pane of glass to see and control these virtual and physical devices.

Q: LOOKING BACK, WHAT ARE SOME SIGNIFICANT SUCCESSES AND CHALLENGES IN YOUR CAREER?

Twenty-six years in the industry has given me a lot of perspective. Challenges have come in the form of technology shifts, cost-cutting exercises, acquisitions and divestitures.

I am most proud of being a CEO in the late 90s of one of the pioneers in the managed security services market. For me, looking across the cybersecurity industry and seeing so many talented and successful people that I have worked with, mentored or have been mentored by, makes it all worth it. This industry matters more than ever before, and I love being part of the community that is committed to protecting the digital world we rely on.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

ED FERRARA
CISO, CSL BEHRING

HEADQUARTERS: King of Prussia, PA

EMPLOYEES: 17,000

ANNUAL REVENUE: $6 Billion

"It is important to remember that information security is one of 500 issues that the Board is dealing with at any one time. We need to have a succinct and clear message to the Board – this is what we are dealing with; this is how we measure it; and this is our path."

- ED FERRARA

It is not uncommon for CISOs to take non-traditional paths to the role, as the industry has only recently emerged. Ed Ferrara's path is just as unique as many of his peers. Ferrara came to the position of CISO at CSL Behring after getting his start as a software engineer, designing new software development processes and methodologies for complex software projects. He became interested in information security because of the poor quality he was seeing in software. It is as most security professionals believe the source of all hacks. Hackers take advantage of software vulnerabilities. Prior to becoming CISO, Ferrara worked in consulting leadership for several global tier 1 consulting companies. Some may recognize Ferrara as the former Vice President and Research Analyst for cybersecurity at Forrester Research.

Ferrara looks back fondly at his time as a Forrester analyst but says he made the jump to become a CISO because he wanted to be more involved in the implementation of strategic security initiatives. He says, "At Forrester, we wrote and researched security topics, but I wasn't doing the dirty work. I wanted to get my hands dirty again, and when the CSL Behring CISO position came up, I jumped at it."

The specific opportunity at CSL Behring has motivated and energized Ferrara. "We are a six billion dollar company providing lifesaving therapies that treat immune deficiency and hemophilia. We are growing fast and that creates its own security challenges. We are growing in parts of the world, like Asia, that require significant security investment."

Ferrara is the company's first CISO and comments, "I am really building the program from the ground up. Before I arrived, CSL had implemented specific security controls,

but there was an inconsistency to the model, so we started with the blocking and tackling first."

Ferrara reports into the CIO, and believes that the Business Technology (BT) organization is the appropriate spot for his security team. He says, "The question of where the security organization should exist within the business is largest a question of maturity. For us, BT is the logical place for my team. Historically, there has been an adversarial relationship between information security and application and infrastructure teams. But we do not have that here. Part of the reason why is because I do not allow my team to say, 'no'. We says 'yes, and let's do it securely'. With this approach, we break down walls and build relationships that make us successful."

"I always use this metaphor," says Ferrara, "The president says to the Secret Service 'I am going to Iraq' and the Secret Service does not say no. It is their mission to allow him to go there safely."

CONFIDENCE IS KEY WITH THE BOARD

"It is important to remember that information security is one of 500 issues that the Board is dealing with at any one time. We need to have a succinct and clear message to the Board – this is what we are dealing with; this is how we measure it; and this is our path."

"This is not the first time I have presented to a Board. I think that Boards are really good at taking a read of the presenter. If the presenter is confident in their data, and projects confidence that he knows what he is doing, then the Board will not have too many questions. Of course the Board also relies on the CEO and COO to assure them that they should place their confidence in this person."

MANAGING ALL THE NOISE

There has been a massive and nearly unprecedented influx of spending from venture capitalists in security startups and as a result, noise in the market. Every vendor touts the next big solution. These startups combine with increased political chatter about cyber security and front-page hacks to create an awful lot of noise and potential distractions. Many CISOs have found it difficult to keep focused on their strategy and execution.

Ferrara says, "This is something I talked a lot about at Forrester with other analysts. We would get a lot of calls from threat intelligence vendors. Threat intelligence is great as long as it is actionable, but if you have all that data and can't do much with it, then what is the point? But the VCs see this as a growth industry. There are lots of smart people studying threat-scape and coming up with ways to protect and defend. At the end of the day the customer needs to do a lot of due diligence. Speaking as a former analyst, I can say that due diligence means doing more than just reading the analyst report and buying the recommended technology. Consider how the technology fits within your business model."

Ferrara continues, "The analyst in me dies hard, so I make it a point to do regular research. I read Daily Dave and Krebs. I also do a lot of my own research on specific topics that are important to us, such as cert management and web filtering."

The Best Way to Learn is to Teach

"I teach one course per year at Temple University. It is a Masters level course titled Data Analytics for Computer Audit and Cybersecurity. In the class, we use big data techniques to find adverse behaviors, such as expense fraud or finance fraud. We also look at cybersecurity. The interesting thing about the class is it combines students from two tracks – audit and cybersecurity – they learn from each other. Fraud detection is all about understanding patterns of behavior, which is where a lot of cybersecurity is headed. Teaching is more than a hobby for me, it's the best way for me to stay current and continue learning."

The Risks and Benefits of Decentralized Information Security

By Stephanie Hadley
Marketing Content Manager

Information security organizations at large enterprise companies are increasingly debating the merits of running centralized or decentralized information security programs. This is an issue for global companies, healthcare conglomerates, umbrella organizations that manage several brands, and even large university systems that have traditionally given autonomy to departments and schools.

TODAY'S REALITY

Today, most CISOs work in hybrid decentralized organizations where business departments have autonomy over specific solutions that help meet their business goals, but operational functions, such as HR and IT, work within a centralized model.

For example, within a large healthcare system hospitals and healthcare providers may make their own strategic business decisions, but IT functions, including hardware and platform decisions are standard across the system. The fact is, information security needs to be involved in all aspects of business and risk management, and therefore IS needs to have a strong presence in every part of the organization, even in highly distributed environments like healthcare systems. Therefore, a completely centralized model that works for the IT organization may not work for information security.

Many CISOs have created centralized information security teams that work well within their decentralized organizations. These CISOs leverage informal partnerships, such as Security Ambassadors to ensure security is represented all the time. Security Ambassadors are non-technical employees outside of the IS team that are trained and deputized to be the security advocate to their part of the organization. These programs allow centralized information security teams to succeed in decentralized businesses. Corey Scott, the CISO of LinkedIn created a Security Champions program to foster inclusion and commitment from outside of the security team.

THE TOUGH QUESTION

The real question for CISOs is how

decentralized organizations can manage and respond to risks, and if risk can be effectively mitigated with a centralized security approach.

When decisions about risk are made at the organizational level in a centralized model, all risk is more easily understood, defined and measured. Yet, this approach also requires that all parts of the enterprise meet a single set of standards, which can be clunky and cumbersome, and sometimes stifle innovation unnecessarily.

Audry Agle, who was previously CISO at First American Corporation and is now at Black Knight Financial Services wrote about the benefits of managing risk in a decentralized environment at CSO Online. She wrote that in a decentralized approach each business unit takes responsibility for its own program. "As [each business unit] will develop their own policies and standards, they are far more likely to embrace the program, assign the necessary resources to it, and fully implement. Rather than having a generic set of policies that can apply across the organization, this model has the advantage of producing policies that are aligned with each unit's specific business model. Further, the business unit can act autonomously, and thus theoretically more efficiently when policy changes or incident investigations are necessary."

While ownership and understanding are potential benefits to the decentralized model, new risks and challenges also arise as a result of the approach. For example, when risk is managed via a decentralized model, careful communication and planning is needed to ensure risks are not transferred from one organization to another without awareness or consent.

5 Benefits of a Decentralized Security Model

1. Employees take greater ownership of risk
2. More awareness of information security company-wide
3. Can enable faster innovation
4. Greater autonomy to achieve business goals
5. Information security is embedded within each department

And 5 Challenges

1. No consistency across the organization
2. Requires stronger and more consistent communication
3. Risk can be overlooked or mischaracterized
4. Still requires strong central support and guidance
5. Requires more staff

Defining Decentralized and Centralized Governance

Bob Turner, the CISO at the University of Wisconsin Madison shared a presentation on SlideShare that provides a good definition of the difference between centralized and decentralized approaches to organizational structure.

Decentralized Governance

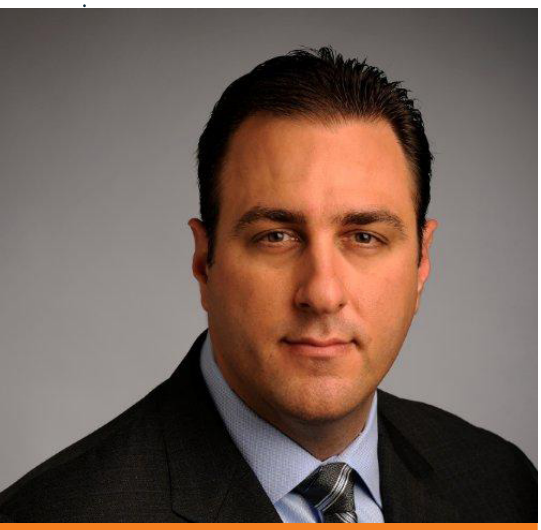
In Turner's description, a decentralized organization, "authority, responsibility and decision-making are delegated to individual groups and teams." He writes that teams establish their own standards, policies and guidelines, and they manage their own cybersecurity risk based on their business strategies. Coordination and communication is necessary amongst subordinate groups, especially to manage and transfer cyber security risk.

Centralized Governance

Conversely, according to Turner, centralized governance includes, "single threaded authority, responsibility and decision making power." Centralized governance involves the entire enterprise in the development and implementation of risk management and cyber security strategies.

Q&A WITH MICHAEL FEY

PRESIDENT & COO, SYMANTEC



Michael Fey is an accomplished enterprise security executive with a highly technical background and more than a decade of cyber security experience. Prior to joining Symantec and Blue Coat, Fey served as CTO of Intel Security and General Manager of McAfee Corporate Products.

SYMANTEC ACQUISITION OF BLUE COAT

It's amazing for people to realize the new Symantec is doing things never done before and running at a speed that few have ever run.

The response we've had from market has been nothing short of astonishing. There aren't many organizations that have spent $4.5 billion and upon announcing IPO, their stock rises to over $5 billion, making the acquisition essentially pay for itself in 24 hours. We've grown the market cap by 8 billion in no less than 6 months.

THREAT TELEMETRY + NETWORK AND CLOUD SECURITY

By combining Symantec's leading threat telemetry with Blue Coat's network and cloud security, we provide customers with unrivaled threat protection and unmatched cloud security.

What's most important now six months in is that our products and ability to service them are getting stronger. The actual technology behind our products has greatly improved since being acquired.

We've acquired LifeLock, integrated the Blue Coat and Symantec product line in 30 different tangible examples that our customers are implementing in the field, we've merged sales forces, and increased retention rates across the organization. At the same time, and under all of that change, our people want to work here more today than they did six months or a year ago. For this, I'm very proud because customers are sensing and seeing a new energy and tenacity from us. Customers need the biggest company in cyber security to be firing on all cylinders. We don't see an end in sight from improvements and impacts we can have on the industry.

SYMANTEC IN 2017

We have the largest set of integrated offerings in the cloud, bar none. What we are showing to the world is how they can embrace the cloud generation and deliver better security posture in the process. We have a platform that can help define the future of cyber security in a way that provides long term sustainability and capability to our customers.

We spend a lot of time working with organizations to help them understand how they can take a traditional defensive posture and embrace the cloud generation in order to deliver more ROI back to the business and become more meaningful. Many organizations are afraid of what data goes in the cloud and the things that could impede performance for the business, which is something we spend a lot of time helping customers understand.

BOARDS & CISOS

The duality role that defines the cloud generation is a challenge to CISOs. They are trying to adopt the cloud, but still deliver great cyber security.

The CISOs who are most meaningful to organizations will set up strategies that allow their companies to accelerate cloud adoption. They know what they want to have in place and are setting up micro-environments where they can embrace a fully cloud-centric world. They realize the necessity and are spending budget and time to get their organizations positioned correctly.

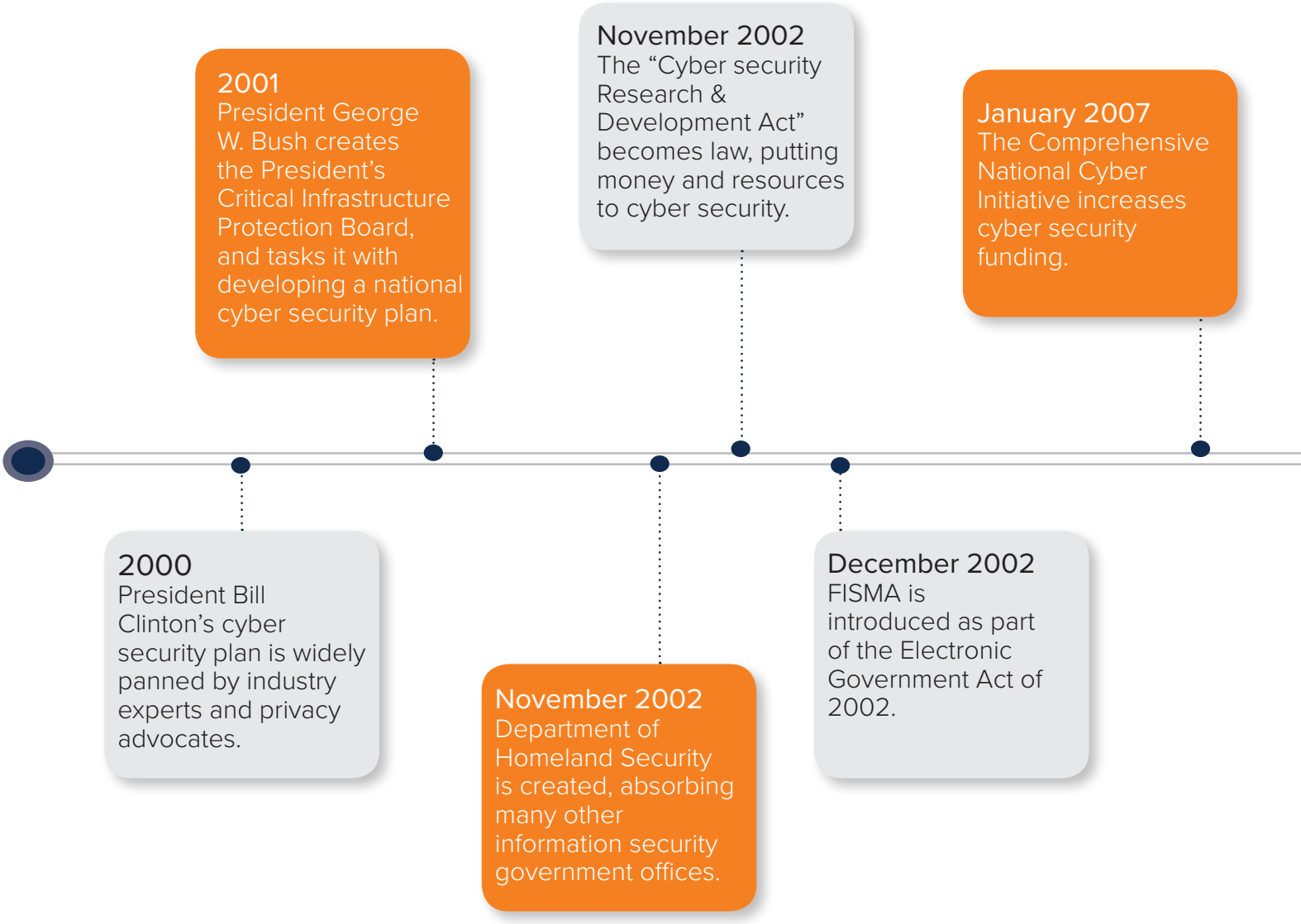
We help define a true strategy for CISOs' defensive posture through building a layered defense model that can react and be nimble while still strong and resilient. We help boards understand the long term strategy for the evolution of a security posture. Even with all of this, we still demonstrate how to deliver a strong ROI. We are not just a runaway cost schedule for cyber security because we can get to a predictable spend model that fits inside most organizations' budgets, and still deliver on a high-end security roadmap.

WASHINGTON'S CYBER SECURITY AGENDA

By Stephanie Hadley, Marketing Content Manager

In 2016, cyber security, long the under-funded, misunderstood, and under-prioritized issue of the day, rose to prominence in Washington and in the general press. Whether we have Clinton's email server or Trump's Twitter account and personal cell phone to thank (or blame) for the rise in cyber security awareness, finally in 2017 the government is poised to get serious about cyber security.

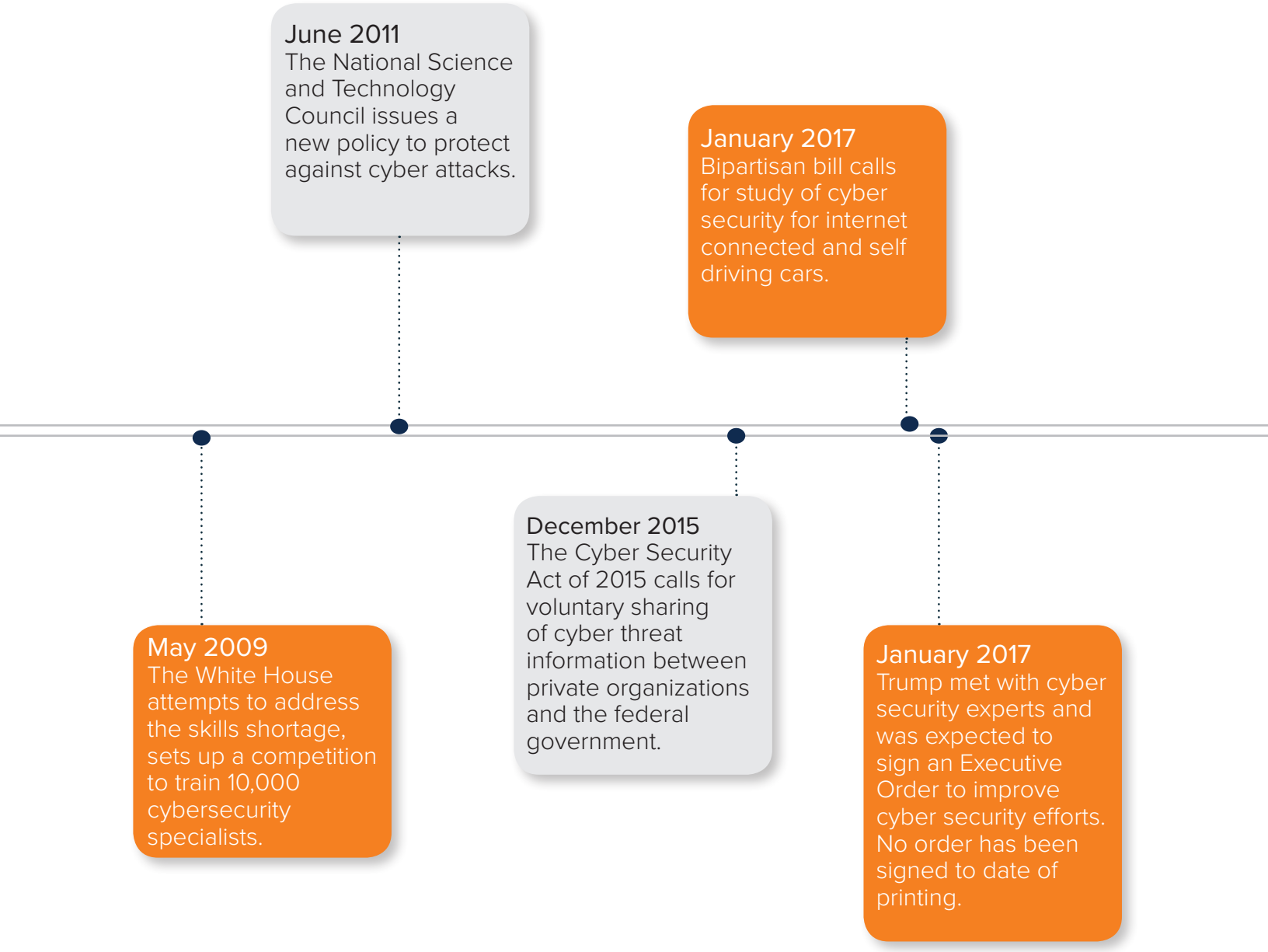
How did we get here, and what can we expect for cyber security in 2017?



On the Congressional Agenda

Russia
Investigations and response to Russian hacking in the Presidential election of 2016.

FISA Section 702 – Renewing Section 702 of the Foreign Intelligence Surveillance (FISA) Act, otherwise known as FISA. This Act allows the U.S. government to conduct intelligence gathering operations aimed at foreign persons located abroad.



ABOUT
FEATS OF STRENGTH

Feats of Strength is a business-focused information security security magazine.

We provide a platform for a diverse set of industry leaders to share their success and challenges.

By connecting people with thought leadership content, we examine different ways to build a confident security programs.

To learn more about the magazine, or to be featured in our Profiles, please go to www.klogixsecurity.com/FeatsOfStrength

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

TRENDS

MARCH 2017

K logix

WWW.KLOGIXSECURITY.COM
888.731.2314