CYBEROREGON

News Release

Experts Outline Cybersecurity Predictions for 2018

Oregon Cybersecurity Advisory Council members and other cybersecurity experts share insights on what's in store for the coming year

Portland, Ore., January 30, 2018 — With the massive data breaches of 2017 in the rearview mirror, what cybersecurity headlines and developments can Oregonians expect in 2018? Building on the launch of Cyber Oregon in November, top cybersecurity experts and members of the Oregon Cybersecurity Advisory Council say it's imperative that business leaders learn from the events of the past year, strengthen community involvement and continue to build awareness about cybersecurity issues.

Among the leading voices is Kerri Fry, Chair of the Oregon Cybersecurity Advisory Council and President of Redhawk Network Security, who says it's important for community members to put aside their differences and join in a common fight against cybercrime. "Where the rubber meets the road is when we break out of our 'comfortable' communities and stretch ourselves—with competitors or cross-sector industries," says Fry. "The common thread is the protection of information. In each industry, we all have information to protect."

Despite ongoing advances in cybersecurity technologies, Charlie Kawasaki, Vice Chair of the Oregon Cybersecurity Advisory Council and CTO of PacStar, predicts many more attacks and data breaches in 2018 and beyond. Here's why: "At a recent conference, I asked an audience of 80 enterprises how many had fully deployed multi-factor authentication, and not a single hand was raised. It's indicative that our community has a long way to go to secure our systems."

Perhaps not coincidentally, Mark Cooper, President and Founder of PKI Solutions Inc. suggests that 2018 is a great year to implement proven technologies like two-factor authentication. "By leveraging two-factor authentication, a stolen or guessed password alone won't be enough to access your critical accounts."

Social engineering ramps up

Speaking to the need for a renewed focus on the role of the human in enabling and preventing cyber attacks is Lewis Howell, Founder and President of Hueya, Inc. Howell predicts that in 2018, hackers who are "armed with relevant, timely, and accurate information" will launch a "myriad of social engineering attacks that will result in the loss of money and reputation."

Like Howell, Fred Cobb, Vice President of Services with Sword & Shield, sees securing the human as a top concern. "Company staff is and will remain the weakest link when it comes to securing a company's sensitive information," Cobb explains. "Social engineering attacks designed to take advantage of human weakness and the good nature of your employees will continue to be used by cyber criminals to steal sensitive information or to distribute ransomware and other forms of malware."

Fiduciary responsibility

On the upside, however, the high-profile attacks of the past year will lead to more Oregon-based firms acknowledging that their "fiduciary responsibility extends to the protection of data—citizen and customer information," predicts Tom Quillin, CTO Security Economics, McAfee. What's more, he expects to see increased cooperation between cyber professionals and management, but it likely won't happen fast enough to prevent all attacks. "Unfortunately, it is safe to predict that some leaders will awaken to this need too slowly, and their organizations will be compromised."

Adding more weight to the notion that cybersecurity is a shared responsibility is Bil Harmer, who has plenty of insight into the evolving cybersecurity landscape in his role in the Office of the CISO for Zscaler, Inc. The reason, Harmer explains, stems from the fact that cyber attackers are working together too. "I believe we will see the beginning of more complex attacks involving multiple targets. How many times have you had to tell your significant other your passcode for your phone? What if your home assistant device has been hacked and is listening for it?"

Along the same lines, Lisa Buschmann, Solution Director, Cybersecurity at CA Technologies, exhorts companies and governmental organizations to do better in 2018. "The application-based password protection of the past will not be sufficient to protect data, consumers of the data and the personal information contained in the data," she says.

AI Tools Emerge

Andrew Plato, CEO of Anitian, also circles back to the role of the human in lax online security. “Having good security technology is insufficient to prevent attacks,” he says, in part because sooner or later “somebody must monitor all that tech.” Experts like Plato and others see emerging artificial intelligence (AI) tools stepping in to take over at least some of the monitoring role in the coming year, but with caveats.

As Haiyan Song, Senior Vice President, Security Markets at Splunk notes, “While the concept of bringing AI to solve cybersecurity challenges is not entirely new, it’s still in its infancy and not core or mainstream. We see AI’s applicability broadening in 2018. With this expansion, it should not be forgotten that actors on the attacker side have the same access to these technology advancements.”

Little things matter

For the coming year, experts like Multnomah County’s information security officer Dennis Tomlin advise that Oregonians “take care of the little things.” For Tomlin, that should involve “diligence in changing passwords from factory defaults and generally paying closer attention to devices that we take for granted that are a part of our increasingly connected world.”

Zscaler’s Harmer emphasizes the need to get better at current cyber protections while preparing for the future. “I would strongly recommend all Oregonians use some form of password manager and ensure they create new strong passwords for each and every site they use.” As for the future, as people build smart homes and add in IoT devices, he says consumers should “spend a little time learning how to protect and manage that smart home to ensure they stay safe and that their investment isn’t used as a weapon.”

Another reason to pay close attention to personal cybersecurity is avoid ransomware attacks, which to date have mostly involved holding networks or data hostage. That could change, says Rob Wiltbank, CEO of Galois, Inc. “Ransomware will start to get personal and target your IoT devices. It’s completely possible that your car could get hijacked by a hacker, preventing you from starting it, until you pay the price with…wait for it…cryptocurrency.”

About Cyber Oregon

Cyber Oregon is a statewide initiative powered by a public-private consortium of technology companies, educational institutions, state/local government agencies, law enforcement and other organizations to build tangible solutions to protect the digital lives of all Oregonians. The

Oregon Cybersecurity Advisory Council was established pursuant to Senate Bill 90, signed by Governor Kate Brown on September 19, 2017, to develop a shared vision for the establishment of a cross-sector Cybersecurity Center of Excellence. The Cyber Oregon awareness initiative was formed in partnership with the Technology Association of Oregon (TAO) to develop and increase awareness of cybersecurity programs, education and resources throughout the state. To learn more about Cyber Oregon, please visit https://cyberoregon.com.

Sponsors of the Cyber Oregon Awareness Initiative include Platinum Sponsors Redhawk Network Security, Splunk Inc. and the Oregon Small Business Development Center Network; Gold Sponsors Amazon Web Services, Comcast NBCUniversal, First Data, Fortinet, and Zscaler; Silver Sponsors Anitian, CA Technologies, Galois, Inc., Hueya, Inc., PacStar, PKI Solutions Inc. and Sword & Shield.

Media Contact
Megan McKenzie or Kelly Stremel
McKenzie Worldwide
meganm@mckenzieworldwide.com
kellys@mckenzieworldwide.com
(503) 470-0197

CYBEROREGON

Quote Sheet

Note to editors: These quotes may be freely used in articles or blog posts with appropriate attribution. Please contact the Cyber Oregon PR team if you would like interviews with any of these cybersecurity experts.

“The European Union will quickly make an example of a large company for failure to meet GDPR regulations. State-sponsored hackers will use artificial intelligence and the scalability of the cloud to wage targeted, highly dynamic campaigns against point of sale and elections systems.”

- **Andrew Plato, CEO, Anitian**

“As we look into 2018 and beyond, citizens and consumers will demand more of their interactions with companies and governmental organizations. At a minimum, at risk continues to be public trust. As new generations freely divulge more and more personal information on social networks, we must find new ways to secure our internal systems. The application-based password protection of the past will not be sufficient to protect data, consumers of the data and the personal information contained in the data.”

- **Lisa Buschmann, Solution Director, Cybersecurity CA Technologies**

“Ransomware will start to get personal and target your IoT devices. It’s completely possible that your car could get hijacked by a hacker, preventing you from starting it, until you pay the price with...wait for it…cryptocurrency.”

- **Rob Wiltbank, CEO, Galois, Inc.**

“In 2018, we will start to see the preliminary impact of the Equifax breach combined with an overwhelming explosion of threats that take advantage of the human factor. Armed with relevant, timely, and accurate information, organized hacker factions will launch a myriad of social engineering attacks that will result in the loss of money and reputation. AI-based cybersecurity products will take a hit as a new paradigm of products focused on securing the human start to address the root cause—turning the tide of cybersecurity.”

- **Lewis Howell, CISSP, founder and CEO, Hueya, Inc.**

“First, business and government leaders will understand that their “fiduciary responsibility” extends to protection of data—citizen and customer information. Unfortunately, it is safe to predict that some leaders will awaken to this need too slowly, and their organizations will be compromised. Second, security professionals will, after ignoring the need for years, improve practices around projecting outcomes and connecting goals to business objectives. This will begin to bridge the gulf between the security community and mainstream management.”

- **Tom Quillin, CTO Security Economics, McAfee; member of Oregon Cybersecurity Advisory Council**

“Nation state actors will increase the targeting of smaller government entities in order to establish a foothold that will allow them to navigate into larger government systems and even gain access to critical infrastructure.”

- **Dennis Tomlin, CISSP, HCISPP, ITIL, Information Security Officer, Multnomah County; member of Oregon Cybersecurity Advisory Council**

“While the technology industry continues to innovate with important new solutions to cybersecurity threats, implementation of even well-known, effective and readily available defenses, procedures and training is still lacking. For example, at a recent conference I asked an audience of 80 enterprises how many had fully deployed multi-factor authentication, and not a single hand was raised. It’s indicative that our community has a long way to go to secure our systems, and as such we should expect to see many more data breaches, malware/ransomware attacks, DDoS attacks and other exploited vulnerabilities in 2018.”

- **Charlie Kawasaki, CTO, PacStar; Vice Chair, Oregon Cybersecurity Advisory Board**

“Attackers are increasingly targeting access to user and company financial holdings. Whether it is online banking access, investment accounts or cryptocurrency, 2018 is the year to focus on improving your authentication to these institutions. By leveraging two-factor authentication (SMS, smartphone app, etc.), a stolen or guessed password alone won’t be enough to access your critical accounts. Ask your financial providers about their offerings and consult independent tracking sites like https://twofactorauth.org/ on where two-factor is available.”

- **Mark Cooper, President and Founder, PKI Solutions Inc.**

"Ultimately, I think the cybersecurity community understands that collaboration is important. We tend to collaborate within the community we are most comfortable with. Where the rubber meets the road is when we break out of our “comfortable” communities and stretch ourselves--with competitors or cross-sector industries. For example, the financial sector has a lot to teach about security. The common thread is the protection of information. In each industry, we all have information to protect."

- **Kerri Fry, President, Redhawk Network Security; Chair, Oregon Cybersecurity Advisory Council**

“While the concept of bringing Artificial Intelligence (AI) to solve cybersecurity challenges is not entirely new, it’s still in its infancy and not core or mainstream in most environments. We see AI’s applicability broadening in 2018. With this expansion of machine learning and AI for cybersecurity defenders, it should not be forgotten that actors on the attacker side have the same access to these technology advancements, and are collaborating and sharing to innovate faster.”

- **Haiyan Song, Senior Vice President, Security Markets, Splunk Inc.**

“Biometric hacking that can circumvent biometric security controls, including those found on electronic devices such as Apple iPhones, Galaxies and Microsoft Surface laptops will increase.”

- **Fred Cobb, Vice President of Services, Sword & Shield**

“Cryptocurrency will be tested in 2018, both through new style attacks and previously experienced stock market scams. Cryptocurrency has just stepped into unregulated stock market territory. Cryptocurrency is completely unregulated, difficult if not impossible to track, and global. There are thousands of people that know how to work the system in the current stock market. Now, take the rules off and see what happens.”

- **Bil Harmer, CISSP, CISM, CIPP, Office of the CISO, Zscaler, Inc.**

# # #

Media Contact
Megan McKenzie or Kelly Stremel
McKenzie Worldwide
meganm@mckenzieworldwide.com
kellys@mckenzieworldwide.com
(503) 470-0197