Why Prevention Still Matters

THE CYBERSECURITY APPROACH YOU CAN'T ABANDON

nuix

INDUSTRY PERSPECTIVE

Introduction

The recent breach of the Office of Personnel Management data affected 22 million records, but its ramifications are even more far-reaching than that. Media coverage of the event ensured that many more people worldwide are aware of the U.S. government's cybersecurity shortcomings and those people are demanding a swift response.

It's in this very public environment that cybersecurity professionals find themselves today, forced to shift their focus from proactively securing the infrastructure to incident detection and response. It's also in this context that a dangerous precedent is emerging, one that preaches the idea that because security measures aren't foolproof and cyberattacks will happen, it's more important to focus on reaction than prevention. The reality is that skimming over and skimping on prevention will only lead to more breaches. The statistics back this up—federal network cybersecurity incidents were up 15 percent in fiscal year 2014 compared with the previous year, according to the Office of Management and Budget.

So what can be done? "The best defense against cyberthreats to government networks lies in a long-proven source," said Chris Pogue, Senior Vice President of cyber threat analysis at Nuix and former U.S. Army Signal Corps Warrant Officer. It ultimately amounts to a two-pronged approach:

- Military-based defense tactics
- Public-private partnerships

GovLoop teamed up with Nuix, a company vthat produces a software platform for indexing, searching, analyzing, and extracting knowledge from unstructured data, and provides tactical solutions to complex business problems, on this report to dive deeper into one of today's hottest topics: cybersecurity. Nuix helps companies understand the impact of cybersecurity threats by offering tactical solutions to complex business problems. To understand the complexity of cybersecurity and then simplify it, we will look at:

- Why cybersecurity's paradigm is shifting
- Mistakes that IT administrators are making when it comes to prevention, detection and response
- How shortages in the number of skilled workers are affecting the government's cybersecurity capabilities
- What cybersecurity approaches are worth the government pursuing

The fact is, cybersecurity is not merely a trend. It's crucial that employees both within and outside the IT department understand the evolving threat landscape and ways to secure against it.

"As defenders, we have to hit every security control every time, all day, every day, and never missing a single vulnerability. All an attacker has to do is find one area to exploit."

– Chris Pogue, Nuix

A Shifting Paradigm

Cybersecurity breaches in the public and private sectors are not new; information and access have long been sought-after commodities by a myriad of ill-intentioned actors – nation-states and insiders alike. What is newer, however, is the attention paid to these attacks, Pogue said.

"We've seen this evolution of companies looking at the perimeter and understanding that they're going to get breached. Organizations like Target and OPM and Home Depot – these aren't small companies, these aren't "mom-and-pops". These are companies that have entire divisions of people dedicated to defending the company's systems. If they can fall down and they can be breached, everybody can."

As a result, it's less shocking to the public to learn that a breach occurred and of greater interest to see how the affected organization will respond. Since the spotlight is on their response, agencies need to manage two windows when a cyberattacker strikes, Pogue said:

- The Window of Intrusion, which is the time between when an organization is breached and when someone discovers it
- The Window of Exposure, which is the time between when the breach is realized and when it's contained

"As defenders, we have to hit every security control every time, all day, every day, never missing a single vulnerability. All an attacker has to do is find one area to exploit," he said. "I think everyone realizes this isn't the most realistic expectation in the world to have, but you can position yourself to identify that a breach took place and react to it as quickly as possible."

"That's the reason for the shifting paradigm," Pogue said. Even recent legal actions by the government reinforce planning for a response. For example:

- In August, the Third Circuit Court of Appeals ruled in Federal Trade Commission v. Wyndham Worldwide Corp. that the Federal Trade Commission can sue organizations for letting hackers access their information. This is based on Section 5 of the FTC Act, which states that the commission has the authority to take action against companies that engage in unfair or deceptive acts that are not reasonably avoided by consumers.

> "You have to strike a balance between prevention, detection, and response."
>
> **– Chris Pogue, Nuix**

- In June, news outlets including Reuters reported on inquiries by the Securities and Exchange Commission into companies' data breaches. SEC officials suspect a new form of insider trading.

This post-breach litigation has created an impetus to push recovery not only to bounce back from loss of customer confidence and market share, but also to avoid lawsuits.

"Now you have regulatory bodies coming after those organizations for not preparing themselves for what is logically inevitable. You are both the victim and the criminal," Pogue said.

When government agencies are too focused on one end of the cybersecurity spectrum, they put themselves at risk.

"We've been harping on organizations to not put all of their eggs in the prevention basket for years," Pogue said. "If the bad guys circumvent the perimeter, then what? That's where the birth of the term 'candy bar security' has come from. It's not a new term, but it means that your security is crunchy on the outside and chewy in the middle because everyone focuses on the perimeter and doesn't think, 'What happens when the bad guys breach the perimeter?' When that happens, you're really in trouble."

"What's more, overlooking the prevention aspect of cybersecurity isn't a smart approach," Pogue said. "You have to strike a balance between prevention, detection, and response."

"It's not a good idea to say since you can't prevent, that you should stop trying to prevent," he said. "I think where organizations need to get smarter is in how they prevent."

In recent years, penetration testing and threat simulations—two important methods of prevention—have become commoditized. The problem is that this results in unrealistic threat assessments that provide an incomplete perspective of your security posture. Compliance with regulations such as Payment Card Industry data security standards, the Financial Services Modernization Act of 1999, and the Health Insurance Portability and Accountability Act is driving this formula.

"Everyone has got a checklist and they're trying to check all the boxes to get their gold star, but that's not really how bad guys operate," Pogue said. "They don't care about checklists and getting a gold star means really nothing to them, so companies should move away from that commoditized type of testing where it's largely a validated vulnerability scan with some human intervention, because that's not a real [penetration] test."

The Right Approach

"The pitfall is not overlooking prevention but thinking it's too simple," Pogue said. "The paradigm is completely wrong and we need to turn it around. There is no technology that is going to prevent an attack. We're very clear on that. You will not automate your way out of an attack."

"But what you can do is called defense-in-depth," he said. "It's where you have multiple components that are part of your defensive posture that work together as part of a strategic plan to defend your critical resources. You can't have one piece or two pieces and expect to call that a comprehensive strategy."

These components include antivirus programs, firewalls, intrusion-detection/prevention systems, web application firewalls, and security information management solutions.

More specifically, Pogue recommended an approach called OPFOR, or opposing forces, which he used during his 13 years in the military. It involves training in an environment that simulates the battlefield.

Translated to cyber defense, OPFOR means identifying vulnerabilities and removing them before the enemy has a chance to exploit them. It also means running through post-attack scenarios by conducting After Action Reviews (AARs) to minimize the element of surprise, and implement valuable lessons learned. No matter how much money or time an agency invests in cybersecurity, if employees aren't trained properly on both prevention and response, they won't know how to act in a real crisis.

"You need to have a mechanism in place that will allow you to replicate the threat landscape, and emulate threat actors. This will help you to align as closely as possible with what the real bad guys are doing, which in turn will help you build a more robust and comprehensive security posture rather than checking a box and getting a gold star," Pogue said.

Going through exercises with a contracted attacker—someone an agency hires to find its holes—provides many benefits, such as:

- Not being beholden to the organization to "play nice"
- Identifying the weak spots and demonstrating exactly how real-world attackers could exploit them
- Itemizing what needs to be secured
- Pinpointing how an agency needs to adjust its response strategy

> "Prevention methods and prevention technologies really aren't any different now than they were years ago. A bit more intelligent sure, a bit easier on the eyes, but they're still not being employed properly."
>
> **– Chris Pogue, Nuix**

"All of that hinges on the ability to undergo those realistic attack scenarios," Pogue said. "You can spend the money, you can have an incident response plan, you can 'do all the things,' but if the first time you actually fire up your incident response plan or employ some sort of countermeasure is during a real attack, you're in big trouble because there is no way you're going to be effective. That's why in the military, we train over and over and over and over again until we're sick of it, because once you get in the theater, you have muscle memory; your training kicks in and you don't think about it. You know how to shoot, move, and communicate."

This requires a cultural change in government—and a little bravery.

"We have no shortage of data, there's no shortage of attacks, no shortage of lessons learned. You just have to be smart enough to realize what those lessons are, implement them, and stop following the status quo," he said. "Remember, conventional wisdom is always wrong."

"Emerging technologies mustn't intimidate IT administrators when it comes to cybersecurity," Pogue said, because this OPFOR, defense-in-depth protection philosophy is the same regardless of whether you're securing network-attached storage, storage-area networks, mobile devices, the cloud, or others.

"Prevention methods and prevention technologies really aren't any different now than they were years ago. A bit more intelligent sure, a bit easier on the eyes, but they're still not being employed properly. Organizations still aren't undergoing that rigorous real-world testing like they should, and so the evolution of technology is going to make it easier to implement, easier to gain visibility into these attack vectors, easier to extract telemetry from disparate data types," Pogue said. "We're circling back to the same core problem: If the decision-makers and the people who are setting up the architecture and the security strategies don't look at all of that and don't put a strategic plan behind it, it's still not going to make a difference."

Workforce Woes

How Nuix's Cyber Threat Analysis Team Can Help

The battle to attract skilled cyber warriors to public service will be ongoing. Until the government can compete with the salaries and "work from home" flexibility the private sector offers to such workers, other solutions are necessary. The best one is to call a truce and form public-private partnerships.

"There are a lot of organizations out there that do want to do the right thing," Pogue said. "Nuix among them. Trust is a crucial element of these relationships. They can't be based on political favors."

"If we can focus on right people, right skills, right mission, then you're going to come out with the right results."

"Having the right tools isn't enough," says Ryan Linn, Director of the Advanced Threat and Countermeasures team at Nuix. "The best tools in the world won't be effective if there aren't trained and skilled individuals working with them. During OPFOR exercises, delays in attack detection lead directly to an increased likelihood of data exposure. Having the right people looking at the right data helps companies respond when it really matters."

> "Attackers aren't like Santa Claus, they don't come once a year."
>
> **– Chris Pogue, Nuix**

OPFOR tactics are a core part of the Nuix Cyber Threat Analysis Team's (CTAT) approach to boosting agencies' cybersecurity. In the past decade, team members have worked onsite and remotely to help hundreds of organizations in six main areas:

Digital forensics and incident response (DFIR)

This involves the investigation into cyber crimes and how affected agencies respond to those crimes.

Attack preparedness.

CTAT helps agencies prepare response strategies, customize incident response plans and conduct first responder training and mock exercises.

Penetration testing.

This involves intentional attacks on computer systems to find weaknesses. CTAT does this for Nuix clients or others who need advanced or DFIR assistance, and it provides the team with a unique perspective from which to advise customers about security architecture, software deployment, and attack preparedness.

Attack simulation.

By giving agencies a chance to engage in simulation exercises in a controlled environment, CTAT lets them see how actual capabilities line up with written strategies and plans. This tactical solution also helps organizations learn the correlations between the alerts they are seeing through their detection capabilities and human activity.

Malware reverse engineering.

Attackers collect data from their victims via malware. CTAT's reverse engineers have been able to find, disassemble, and decode some of the most complex malware on the planet, helping government and law enforcement agencies understand the nature of the infection, how to find it on their systems, how to eradicate it, and how to defend against it.

Intelligence acquisition.

Using artifacts from the previous actions, CTAT can find threat patterns and attacker trends, information that agencies can use to find cybercriminals. This data can also help in FTC and SEC inquiries by showing exactly what was exposed.

"Attackers change tactics based on what defenders are doing," Linn says. "We have to be training and testing with the latest in attack trends to make sure that the existing tools, techniques, and training are sufficient to ward off and identify today's attacks. Defenders will always be behind, but regular training and testing helps them trail more closely to understand the threats and respond faster." Nuix's tactical offerings aim to help answer that need.

"We will evaluate an organization's capability to deflect, detect, react, and respond to a realistic attack," he said. "Hopefully we're the ones who find, through testing, the shortcomings, but sometimes it's the bad guys—yet the lessons learned are no different."

A crucial part of CTAT's role is continuous security assessment. To that end, Nuix can maintain its tools on an agency's network if it opts for ongoing testing.

"Attackers aren't like Santa Claus," Pogue said. "They don't come once a year. CTAT goes beyond testing; it partners with customers to perform continuous assessments. Nuix can maintain tools on an agency's network to test as often as changes happen. This allows organizations to find out that they have introduced problems before an annual review and ensure that changes haven't inadvertently introduced new vulnerabilities. CTAT can also use Nuix tools to capture volatile data, gather forensic images, dump memory and generate packet captures for incident response. All of these services together create the recipe for effective cybersecurity incident response."

"It's that holistic solution, not one in lieu of the other," Pogue said. "And all of that hinges on the intelligence of understanding the threats, understanding how attacks take place and why they take place—sort of all that field-operative, 'James Bond,' out-in-the-real-world-type information. When you have that, it becomes so much easier and so much more effective to develop strategies to defend against attackers. Without that, you will never, ever successfully defend against the actors in the current threat environment."

Conclusion

A recent shift in attention to incident response and away from incident prevention is putting the government's cybersecurity at risk at a time when public confidence is already low. In the battle to defend against cyberattacks, public and private sectors need to combine their knowledge to engage attackers more quickly through using the right tools, the right training, and intelligence about emerging threats to help detect, deflect, and respond to attackers before they can cause harm.

"If you don't challenge the status quo and you don't do the things that need to be done, nothing is ever going to move in a new direction," Pogue said. "I think that's really where we need to see heels being dug in and see experts making these decisions, not politicians, not lawyers."

"The right people plus the right technology will yield the right results," he said.

"It's always a combination of technology and people; never ever, ever, ever one in lieu of the other, and the better you get at figuring out how to optimize those, the more effective you can be as a team in helping these organizations prepare themselves," Pogue said. "We're trying to hit that perfect combination of the best people with the best technology. In my opinion, this is going to be game-changing."

> "If you don't challenge the status quo and you don't do the things that need to be done, nothing is ever going to move in a new direction."
>
> **– Chris Pogue, Nuix**

About Nuix

Nuix protects, informs, and empowers society in the knowledge age. Leading organizations around the world turn to Nuix when they need fast, accurate answers for investigation, cybersecurity incident response, insider threats, litigation, regulation, privacy, risk management, and other essential challenges.

Nuix makes small work of big data volumes and complex file formats. Our solutions combine advanced technology with the extensive knowledge of our global team of industry experts. We bring data to life with clarity and intelligence to solve critical business problems, reduce crime, and secure and manage information.

About GovLoop

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 200,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to: Catherine Andrews, GovLoop Director of Content, at Catherine@govloop.com.

www.govloop.com

@GovLoop

1152 15th St NW, Suite 800
Washington, DC 20005

Phone: (202) 407-7421 | Fax: (202) 407-7501

www.govloop.com
@GovLoop