MANAGE

Build a proactive cybersecurity approach that delivers

Whether it's zero-trust, adaptive security or just plain common sense, IT leaders must embrace an approach to IT security that's proactive, not reactive.

Stan Gibson
Stan Gibson
Communications

It's not your imagination. Smart and resourceful bad actors are out to get your organization's data. You've got to do something. You've heard about proactive cybersecurity strategies like zero trust, but what does *zero trust* really mean, how much will it cost and where do you start? Whatever the strategy, the first step for IT leaders is to come to grips with the threats their organizations are facing.

"We're under constant attack. There are millions of hits. We assume we're going to be attacked and that there will be something inside or outside," said Joel Garmon, CISO of the University of Pittsburgh.

IT security executives like Garmon understand that perimeter-based security measures are increasingly irrelevant. Stories are legion of organizations that, once penetrated, fell victim to advanced persistent threats, which can abide for months within a firewall, passively collecting information or actively doing damage.

"Just because someone has gotten into a building or network doesn't mean we should trust them," said Don Anderson, senior vice president and CIO of the Federal Reserve Bank of Boston. "Everything we do should be zero trust."

Despite the need for a new approach, zero trust is not for everyone. Implementation takes commitment, time and resources. "You have granular insight into every application and service a user is using. Tactically, however, it's really difficult," said Johna Till Johnson, CEO of Nemertes Research.

"There has to be a good business reason to adopt a zero-trust policy. It's not going to happen overnight," asserted MongoDB CISO Lena Smart, who has responsibility for security within the company's software as well as for MongoDB and its employees.

Needed: A plan, processes, people

At the Boston Fed, Anderson is grappling with high-stakes cybersecurity challenges. In addition to being a repository for large amounts of money in its role as a bank of banks, the Boston Fed audits banks in its region, a process that generates reams of confidential information that must be safeguarded. The bank also is privy to interest-rate decisions by its board that must be kept confidential, lest leaks of interest-rate tweaks set off a flurry of premature market action. Boston is headquarters for the Fed's District 1 (of 12 nationwide), consisting of all of New England except for the southernmost part of Connecticut.


Don Anderson

Anderson must strike a difficult balance, enabling both collegial interaction and airtight, proactive security. "In our community, we have Ph.D. economists from Harvard or MIT. They are used to an open and collaborative organization. Then there are people doing billion-dollar wire transfers who expect the tightest security," he explained.

The institution weathered recurrent distributed denial-of-service attacks for several years but now is most concerned with protecting against attacks and attempted theft by criminals or nation-states. "Many banks hold balances with us," Anderson said. "We would not want money in their accounts to be wiped out."

The Boston Fed began a decade ago to implement a defense-in-depth strategy based on the Cybersecurity Framework from the National Institute of Standards (NIST), a unit of the U.S. Commerce Department. Starting with identifying sensitive data and its location, the framework provides a comprehensive checklist of all the measures organizations should take to protect critical data and applications.

Authentication, segmentation minimize exposure

At the Boston Fed, defense-in-depth begins with stringent authentication. "Not everybody should have access to everything," Anderson said. Two-factor authentication is required of those accessing the network, and users only gain access to the particular applications and data they require to do their work.

At the University of Pittsburgh, Garmon has taken a similar approach, implementing two-factor authentication and least-privilege access. "Least-privilege is as old as security. You give people only what they need."

Blockchain as an identity guarantor

Controlling access to data and applications by verifying user identity is a key component of a proactive security strategy. The hacking-resistant character of blockchain technology has attracted the interest of The Linux Foundation in developing a new "self-sovereign" approach to secure identity management called the Hyperledger Indy project.

"Self-sovereign identity has its place. We are seeing the death of the username and password," said Forrester Research analyst Chase Cunningham.

Hyperledger Indy builds on Hyperledger open source blockchain technologies. The goal of the project is to create a digital identity system that will enable individuals to present verifiable credentials to whomever they want, without relying on a third party. The effort spans multiple industries, including financial services, supply chain, manufacturing and the internet of things.

Chase Cunningham

Operating under the assumption that attacks are occurring all the time, either from outside or inside the organization, the university has broken its data down into chunks to minimize exposure, Garmon said. "We are highly segmented. If a workstation wants to talk to a different server zone, we have to open up the firewall."

The Boston Fed has adopted a similar approach, sometimes called microsegmentation. "You would typically separate out your presentation, application and database [layers] in a three-tier architecture. A user or application can't just reach out and touch one or the other," said Anderson, explaining that specific permission must be granted.

A proactive approach to security in software

Rather than adding security features to an application after it has been written, organizations are adopting DevSecOps, the blending of security measures with the DevOps approach to iterative software development. The result is to generate inherently secure applications in step with today's rapidly evolving digital business strategies.

"For a new application that's being built from the ground up, it's easier to implement security," Anderson said. "Business areas are loving it [DevSecOps] because they are getting [applications] faster."

Smart, a veteran of DevSecOps implementations prior to joining MongoDB, agreed that this aspect of proactive cybersecurity pays dividends. "Developers like to be challenged. Teaching them to integrate security into the earliest stages of the development lifecycle makes their job more interesting." However, she recommends implementing a trust-nothing approach even here, having developers form teams and attempt to hack each other's code.

Shoring up the human factor in proactive security

A comprehensive approach to cybersecurity must incorporate the users themselves as a line of defense, getting everyone involved in the effort to identify and defend against attacks. "I hate calling customers and staff *the weakest link*. They are the first people who might see something wrong," Smart said. "A proactive approach and being transparent means having an open ear to people who want to talk about security."


Lena Smart

At the Boston Fed, background checks are de rigueur for new employees. Once hired, employees get a security briefing, which is followed up by random tests in which an IT staff member sends out fake phishing emails and rewards those who report them. The institution remains on guard for insider risks, studying employee behavior for any unexpected changes, a process known as *user and entity-based analytics* (UEBA). For example, if an employee who normally logs off the network and goes home at 5:00 PM instead logs on and downloads large files at 3:00 AM, that behavior would be flagged as anomalous and even suspicious.

Zero-trust advocate

"There are only two types of organizations: those that know they have been attacked, and those that do not yet know they have been attacked."


Stuart Madnick

That's an oft-quoted observation by Stuart Madnick, MIT Sloan professor of information technologies.

Madnick is at the forefront of cybersecurity research, leading initiatives that champion a zero-trust approach to safeguarding data.

"Start off with the premise [that] they are in your system. Think of the worst thing that could happen. Then start looking to see if that is happening. Zero trust puts you in that mindset," he said.

Much is at stake. According to Madnick, the average intrusion has been going on for over 200 days before it's detected.

You are not alone: Information sharing

In the quest to keep bad actors at bay, organizations facing similar cybersecurity challenges would do well to share information as to what works and what doesn't. The Boston Fed gathers monthly with CISOs of some 70 constituent banks to share security concerns. "We talk to banks both large and small about computer hygiene," Anderson said.

At the University of Pittsburgh, cybersecurity experts make the rounds to different departments, giving briefings on threats and defensive measures. In addition, Garmon said, he and his staff take part in cybersecurity activities of Educause, an organization that helps higher education institutions improve their use of IT.

Raising awareness about the university's proactive cybersecurity efforts is also important to gain funding. "We do a heat map, a chart that shows where we're good and where we're bad, and show that to management to highlight gaps we need to fix," Garmon said.

"The goal is to present the risk in a way that is quickly and easily understood. If the risk is high, then funding might be gained. Executives don't want a 30-page report," he explained. In addition to the NIST Cybersecurity Framework, Garmon relies on NIST Special Publication (SP) 800-171, which includes guidance for explaining risk and cybersecurity issues within an organization.

ROI on proactive cybersecurity


Joel Garmon

Assessing payback for a major proactive cybersecurity drive is complicated. "It's not something you can demonstrate easily. But we talk about cost-avoidance. By showing regulatory compliance, we can avoid fines and reputational costs," Garmon said. Other benefits make intuitive sense. For example, protecting data about University of Pittsburgh donors is essential for retaining the institution's major funding sources. "We depend on donors. We can't afford to lose contributor data," Garmon said.

A company starting fresh is likely to have smoother going with zero-trust implementation, according to Anderson. "If you are a new company, it's easier; but with stable applications, you have to re-think." Because of the Boston Fed's far-reaching responsibilities, including the need to safeguard confidential communications and large amounts of money, provable ROI is beside the point. "For a typical bank, there would not be ROI for what we do."

For MongoDB's Smart, however, a clear business case is essential. "There has to be good ROI. We have to explain what it is and why we are doing it."

Johnson of Nemertes agreed that advocacy is essential. "You're going to be a lot more successful if you have an empowered evangelist -- if your CISO is a believer in zero trust and is well regarded in the organization," she said.

Once the case is made, the hard work begins. "It's all well and good to say, 'Yeah, we do zero trust.' But you have to be willing to do the heavy lifting," said Johnson. Anderson agreed. "Implementing it is not easy or cheap. It's a fundamental change that can take years."

Google's BeyondCorp is a zero-trust bellwether

Faced with the increasing futility of perimeter defense, Google rethought security for its own employees and contractors. The result was BeyondCorp, a strategy that implements zero-trust concepts through an application proxy for web-based applications. The architecture does away with a VPN, and according to Sam Srinivas, product director for BeyondCorp at Google, "It just works."

"There is no such thing as an internal application. Everything is just on the internet, so you apply security at the application layer," Srinivas said. Access should be based on user needs. "Know just who the user is and the context around their access -- such as the user name, device and group," he said.

A proactive cybersecurity mindset did not occur overnight. Google began developing BeyondCorp nearly a decade ago and has staged its own migration gradually, eliminating VPN-based access bit by bit. Now, Google offers BeyondCorp's reference architecture to any organization and offers application proxy technology as a service, called *Context-Aware Access*, on the Google Cloud Platform. In addition, the company extends BeyondCorp principles to back-end microservices implementations through Google Cloud Service Mesh. "It's like BeyondCorp for services," Srinivas said.


Sam Srinivas

NIST Cybersecurity Framework roadmap

Few veterans of the proactive cybersecurity journey have traveled without a roadmap. Many have relied on the "Framework for Improving Critical Infrastructure Cybersecurity" from NIST.

"The Fed has been leveraging it for a number of years," said the Boston Fed's Anderson. "It's all-encompassing, open source, and there are a lot of controls in it."

The NIST Cybersecurity Framework does not specify technologies; instead, it discusses how to protect information assets in terms of cybersecurity activities and outcomes in a way that's understandable for nontechnical readers. Whether to follow all or part of it and which technologies to deploy are decisions for proactive cybersecurity leaders in IT to make for themselves and their organizations.

"Any organization can pick it up and use it. Nations can also use it," said Kevin Stine, chief of the applied cybersecurity division of NIST, whose responsibilities include the Cybersecurity Framework.

Although zero trust is not mentioned specifically, Stine said there is conceptual overlap between the NIST framework and zero-trust approaches.

A major Cybersecurity Framework update, version 1.1, was released in April 2018. Its enhancements include increased detail on identity and access management, including two-factor authentication. The framework -- which, like all NIST publications, is downloadable and free -- is but one of a number of NIST initiatives and activities focusing on cybersecurity and related fields.

Other NIST initiatives on security and privacy

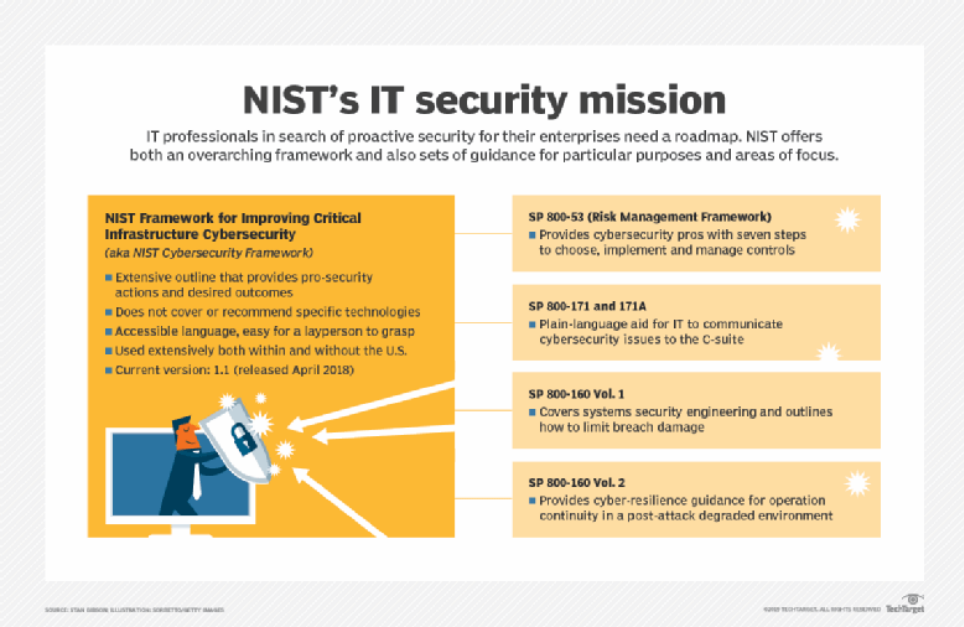
- Collaborating with the federal CIO Council to apply the zero-trust approach to federal information systems.

- A forthcoming Privacy Framework that will help organizations secure personally identifiable information.
- A forthcoming report on cybersecurity for the internet of things that will be part of the Cybersecurity Framework.
- Work on the NICE initiative that promotes the education and training of IT specialists, among others.
- Work to maintain American leadership in artificial intelligence.

NIST has also created a Risk Management Framework, also known at NIST as SP 800-53, under the leadership of Ron Ross, computer scientist and NIST fellow. The Risk Management Framework is a seven-step process to help organizations choose the right controls, implement them and be accountable.

Additionally, there are other guidelines of relevance to IT that NIST has authored (see image "NIST's IT security mission").

TECHTARGET



Other proactive cybersecurity frameworks

In addition to NIST, a number of different organizations are active in formulating guidelines to protect data against attack and theft. Consultancies Forrester Research and Gartner have both come up with frameworks for their clients to follow. Forrester's is called Zero Trust Extended (ZTX), and Gartner's is called Continuous Adaptive Risk and Trust Assessment (CARTA).

Stan Gibson asks:

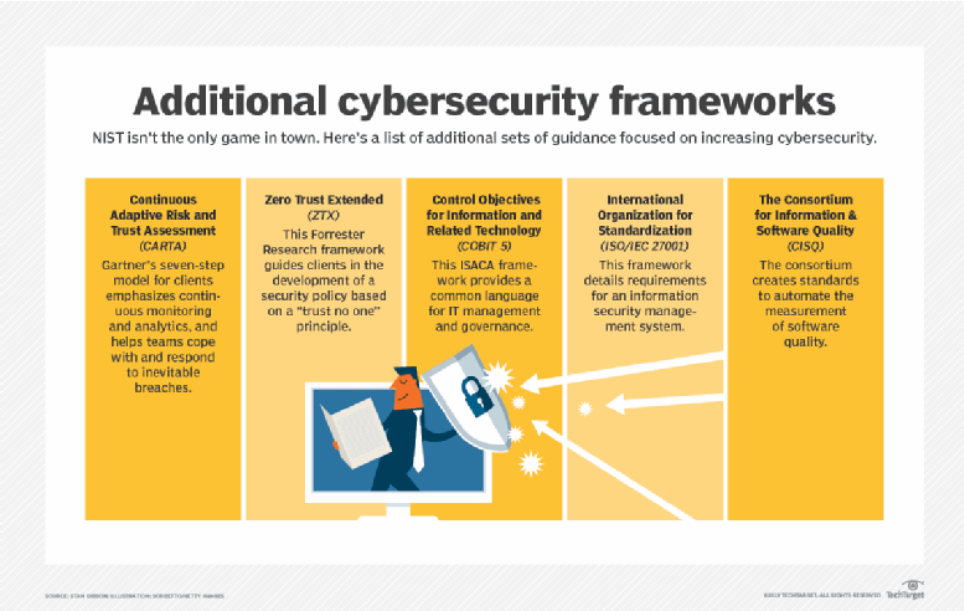
What elements to IT security do you think are most essential to implement first?

Join the Discussion

"There is a difference between compliance [with a framework] and being secure. Being secure is running the marathon -- a multiyear strategy that will pay off in the long run," said Chase Cunningham, an analyst at Forrester Research. In addition to providing clients with a ZTX cybersecurity roadmap, Forrester ranks vendors according to their ability to advance ZTX principles.

The zero-trust slogan was coined by former Forrester analyst John Kindervag, now Field CTO at Palo Alto Networks. "There are a lot of myths surrounding zero trust. For example, there are no zero-trust products. There are only products that work well in zero-trust environments," wrote Kindervag in an email exchange. "Also, zero trust is not the same as multifactor authentication. Multifactor authentication is an attribute used to validate asserted identities that are used to create policies in zero-trust environments," he added.

TECHTARGET



Gartner advocates what it calls *adaptive security* and codified its principles in CARTA. "It's a model for runtime attack protection. Prevention alone is not enough. Despite our best efforts, bad guys get in. So you must have capabilities to respond when they get in," said Neil MacDonald, an analyst and research fellow at Gartner.

CARTA is built around seven steps, with an emphasis on continuous monitoring and analytics, that implement artificial intelligence and machine learning. "Monitor everything you can -- user behaviors, network flows, system behaviors. Determine if something bad has gotten in," said MacDonald, adding, "If things get out of whack, you take action. That's adaptive."

Security pros like MacDonald and Kindervag make it clear that a security perimeter defense is passé today, thanks to, among other things, the prevalence of IoT devices and cloud. But there's no end in sight to the onslaught of breach attempts by bad actors. It's essential that those charged with defending organizational IT systems and data alter their notion of cybersecurity and move from a defensive to a proactive posture. Guided by a cybersecurity framework, or a combination of several, those leading IT strategy must work now to ensure their personnel and processes are revised to meet the cybersecurity threats ahead.


John Kindervag

This was last published in June 2019

Dig Deeper on Risk assessments, metrics and frameworks

- How to perform a building security assessment
- How to conduct a security risk review on a large building
- CERT/CC's Art Manion says CVSS scoring needs to be replaced
- CISOs build cybersecurity business case amid attack onslaught

Load More

Join the conversation

1 comment

Send me notifications when other members comment.

Add My Comment

Oldest ▼

[-] **stangibsonmedia** - 27 Jun 2019 2:23 PM

What elements to IT security do you think are most essential to implement first?

Reply

Latest TechTarget resources

CLOUD SECURITY

NETWORKING

CIO

SearchCloudSecurity

AWS, customers tackle cloud misconfigurations and data exposures

ENTERPRISE DESKTOP

CLOUD COMPUTING

COMPUTER WEEKLY

AWS re:Inforce, the cloud provider's inaugural security conference, addressed the problems of misconfigurations and data ...

Everything you need to know about multi-cloud security

Make multi-cloud security a reality in your organization with these tips and strategies from industry experts as you implement ...