TALKING CYBER SECURITY WITH THE BOARD OF DIRECTORS

/ An interview with Josh Shaul, VP, Web Security Products

Q&A

What are the basics that board members need to know about cyber security today?

Josh: Board members recognize the growing importance of cyber security. Interest and concern are high. That's why it's on their agenda. But they likely have very different degrees of technical background and so are uneven in their understanding of the issues. So when the CIO or CSO reports to the board on the enterprise's cyber security posture, there's usually some education and level-setting to be done.

Board members should first of all have a sense of the threat landscape and how it keeps changing. That includes understanding some basics about types of attacks and defenses. They should appreciate how different attacks — DDoS, malware, web attacks — demand different defenses. Security is complex.

Second, they should recognize that traditional perimeter firewall defenses are inadequate when the business operates online and is highly connected with customers and partners, sometimes around the world. The perimeter has to have openings, but when networks and applications are open to customers, they are also open to attack. Because business has become very distributed, security must be distributed as well.

Third, recognize that there is no such thing as a completely airtight defense. “Is the enterprise secure?” is not a yes-or-no question. The questions to discuss are: Is the enterprise secure enough to operate successfully? How much risk are we willing to accept? How much are we willing to invest to reduce the level of risk?

Fourth, know that success is local. Headlines about major breaches keep reminding us how costly failure can be, and there are lessons to be learned from what happens to others. But cyber security must center on the potential threats and vulnerabilities specific to the enterprise even in the presence of media coverage.

In an ideal world, what would the CIO or CSO like to tell the board regarding the local security posture?

Josh: The discussion would cover three topics — defenses, customers, and response.

Defenses. We have effective defenses. We follow changes in the threat landscape. We have visibility into our digital assets and networks. We’ve done all the diligence we can to protect ourselves from being the next victim of a cyber attack. In addition to perimeter defenses, we have a global shield in the cloud protecting our assets and communications wherever they may be. We are also monitoring inside communications and guarding against inside threats with the same rigor we apply to external ones. And very importantly, we are regularly testing and validating our defenses with “live fire.” We hire expert hackers to try to hack us and immediately fix what turns out to be hackable.

Customers. We’re constantly monitoring our customers’ access to our business, and we want them to have a great — and secure — experience when interacting with us. We understand their normal online behaviors, and we’re carefully watching for any abnormal access. We ensure that it’s really customers who are interacting with our systems, and not bots impersonating them. And we notify customers when we notice that fraudsters may have stolen their credentials or even identities. So we’re protecting our customers, their privacy, and their data, and thus maintaining our customers’ trust.

Response. We’re prepared, even for the worst. Our team is trained. They know how to respond when an attack or breach does occur. We’ve got our game plan laid out, including who we’re going to inform and engage with, including executive management and corporate legal and communications staff. We know how we're going to collect evidence and conduct forensic investigations. We go through realistic incident response exercises. We're not going to be caught on our heels, because we've got our incident response processes locked down, and we've practiced and practiced.

To summarize: We're protected as best we can, we're protecting our customers, and we're prepared, even for the unexpected. Now, you said "ideal world." Not many organizations can honestly say all those things today.

Why not? What's in the way?

Josh: The simple answer is usually lack of funding for a more complete security program. But that's the symptom on the surface. Peel back a bit, and the problem is lack of context and direction. Many organizations have difficulty determining how secure they need to be, or how much risk they're willing to accept, or how much they're willing to spend to get risk to an acceptable level.

To help get over those hurdles, we recommend developing formal statements of the risk appetite of the enterprise. For example, a government agency within the Treasury Department has a fairly low overall risk appetite around technology, which they break down this way:

- No risk appetite for unauthorized access to systems, so controls have to be as tight as possible.
- Low risk appetite around business resiliency, meaning that if systems do go down, they need to come back up soon.
- Moderate risk appetite for using innovative technology solutions to meet user demands, so it's okay to experiment within bounds.

A commercial enterprise operating 24/7 and trying to grow markets around the world would have a very different appetite for risk. The point is to articulate where you stand, to set some useful boundaries, and to get alignment on that. For an area as important as cyber security, the alignment and sign-off on risk appetite should extend across the executive team and the team should make sure the board understands its decisions.

Such statements of guiding principles are a powerful management method. They put stakes in the ground, help prioritize objectives and actions, and provide a basis for decisions. Having agreed on the broad picture set forth in the principles, stakeholders are more disposed to agree, and more willing to compromise, with how the details play out. And those responsible for managing the activities and making tactical decisions — in this case the CIO and CSO — have much firmer ground to stand on, and more convincing ways to explain and justify their actions.

Please say more about how to determine risk appetite.

Josh: It helps to have some external reference points, either industry benchmarks of security practice or more general cyber security maturity models. Trusted third parties can assess an enterprise's security capabilities, and sometimes rough budgets, against industry peers and competitors. The results can identify and justify actions needed, especially to avoid being among the most vulnerable to attack in the industry.

Maturity models organize defenses and operational and management processes into levels of capability, typically five or so. An organization might do an assessment and conclude, "We're at level two and that's too low — we have too much business exposure." The maturity model can indicate what additional capabilities are needed to reach level three. The enterprise's risk appetite statements should drive the maturity level goal.

A useful technique is testing the risk appetite statements with local scenarios and reality checks. For example, an enterprise might at first glance think that it has to serve all its online customers 24/7 without exception. But in the event of a major attack, would it be willing to take down a key system and lock out 30% of its customers to preserve access for the rest?

As another example, the enterprise might want zero tolerance for unauthorized access to its network. But that's an impossible goal, even for the most secure governmental security agencies. In most organizations, such access has already happened and is happening right now. Their challenge is to find and disable the intruders. So, the realistic risk appetite question becomes: What kinds of intrusions do we most need to recognize and contain?

Scenarios like these should be considered ahead of time and become part of the game plan for response. Scenario planning should include putting yourself in the position of the attackers and anticipating what assets may be most vulnerable. If you can help it, you don't want to be making key decisions on the fly while under attack and amid the "fog of war."

The process of developing and testing risk appetite statements is iterative, often centered on costs, and driven by the realities of what it takes to meet security objectives. "We need X level of security." "That will cost $30 million." "Okay, in that case, we can live with less than X." The risk appetite statements may also need to be amended in the wake of attacks, either recognizing the need for better security, or recognizing the reality that the organization isn't living up to its risk profile.

Finally, and very importantly, risk appetite statements can't be generic or theoretical. They must be specific enough to your enterprise situation to guide people in making decisions and tradeoffs, including the most difficult ones.

You mentioned visibility into the computing environment. That must be a foundation for effective cyber security.

Josh: It certainly is. The more complete your visibility — into assets, connections, network activity, vulnerabilities — the better you're able to protect the entire environment. But it's not that simple.

Comprehensive security needs an accurate inventory of the enterprise's networks, systems, and data to begin with, and that's a challenge on several fronts. A common example is the location of sensitive data. Many organizations don't know where all of it is stored. Another is the network surface area of the organization — all of the connections, partners, URLs that might lead into the computing environment. In a large enterprise that has been online for a long time, a complete inventory can be very difficult to take.

Even with a good inventory, an enterprise's visibility into its environment may be incomplete for any of several reasons:

- It may not know where to look or what to look for. In that case, it could use some expert guidance.
- It may not know how to look. In that case, they can also use help from technological tools for monitoring infrastructure.
- It may not want to look for fear of what it will find …

This is a delicate area and perhaps an "inconvenient truth" in the security community. There can be dark corners where organizations don't want to shine a light, because what they find they will then be obligated to fix, and that might prove difficult and expensive. Sometimes it may seem that you're better off not knowing your problem. But that's not the case.

Leaving problems unfound is not okay. Ignorance doesn't serve as an excuse after a breach. However, finding problems and leaving them unfixed can be okay. It's a matter of priorities. No enterprise has the money, staff, and other resources to fix everything. And there's inevitable tension among defensive capability, cost, and business risk. So, we come back to risk appetite. With full visibility and knowledge, you can concentrate on fixing vulnerabilities that carry the greatest risk. The enterprise can then operate comfortably within its risk appetite.

To wrap up, give us the key takeaways for CIOs and CSOs.

Josh: First, when working with the board, cover more than the state of technical defenses and risk of attack. Also discuss customer protection and the preparedness of the security organization and incident response procedures in the event of attack. Together these topics represent thorough due diligence.

Second, the board must understand that the enterprise can never be completely secure. But it can operate within a purposefully determined and acceptable risk appetite. Broadly speaking, the CEO and board should be able to communicate security strategy and risk appetite to the stakeholders — customers, employees, regulators, and shareholders.

Third, security leaders often struggle to get the resources they need to fulfill their responsibilities. Many find it difficult to communicate the business value and necessity of security programs to the financial gatekeepers. It helps to have a regular cadence of communication with the executive team and board about cyber security and risk appetite. The key to unlocking resources may be comparisons with industry peers. But keep in mind the reality that the risk-adjusted security needs may not include all that the security leaders would like to accomplish.

And fourth, when security capabilities and risk appetite are both clear, cyber security programs and processes can help the business set boundaries for action. Security should not just be "thou shalt not," but also "here is your freedom of motion to operate and innovate online." Cyber security staff should be involved early in the conception and development of new business initiatives. Cyber security should enable the progress of the business while preventing the progress of its adversaries.

As the world's largest and most trusted cloud delivery platform, Akamai makes it easier for its customers to provide the best and most secure digital experiences on any device, anytime, anywhere. Akamai's massively distributed platform is unparalleled in scale with over 200,000 servers across 130 countries, giving customers superior performance and threat protection. Akamai's portfolio of web and mobile performance, cloud security, enterprise access, and video delivery solutions are supported by exceptional customer service and 24/7 monitoring. To learn why the top financial institutions, e-commerce leaders, media & entertainment providers, and government organizations trust Akamai please visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter.

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 57 offices around the world. Our services and renowned customer care are designed to enable businesses to provide an unparalleled Internet experience for their customers worldwide. Addresses, phone numbers and contact information for all locations are listed on www.akamai.com/locations.