Why most businesses are not where they want to be when it comes to Cyber Security

by Matthew Goche

Cyber security is making the news every day with headlines of hacks, scams, and data breaches. Yet most businesses are not where they want to be when it comes to cyber security. Why not? The pressure is certainly on. The need is obvious. What's missing?

Let's be clear right from the start: what's missing is not some crucial technological widget or some vital piece of coding. There is no "silver bullet" that would make everything secure. That would be a foolish assumption, since cyberattacks are getting more sophisticated all the time. Even if a "silver bullet" existed today, it would be obsolete tomorrow!

No. The greatest threat to cyber security has nothing to do with technology or the lack of it. It is deeper and more foundational than that. The reason most businesses aren't where they want to be when it comes to cyber security has to do with their *culture*, *perspective*, and *strategy*.

Culture:

Making the Move from Disconnected to Connected

There is a wide disconnect today between the Chief Information Security Officer (CISO) – or whoever in a company plays that role, regardless of their title – and the board of directors or the rest of the C-suite. This disconnect can be seen in three common approaches non-IT executives take toward cyber security:

1. **"Security is a purchase."** Some executives think of security in terms of items: "You say we need a Security Information and Event Management (SIEM) system? A stronger firewall? Some other technical gizmo? If we can afford it, go and buy it. If I buy the item, the security problem will be solved. Next item on the agenda, please."

   Disconnect: This approach doesn't seek to understand what a potential problem and/or solution might mean to the business as a whole. It doesn't weigh the true risk of a threat, or the implications of different security measures on the processes or the people involved.

2. **"Security is a pain."** These executives view security as an obstacle blocking the way of progress and innovation. Every time someone comes up with a great new application, identifies a strategic third-party vendor, or develops a new service or product, IT is there clamoring about security precautions and protection measures.

   Disconnect: Security isn't being promoted as a "win" for the organization, for their vendors, and for their customers. The benefits of maintaining a secure environment aren't understood and/or valued.

3. **"Security is a passing grade."** Executives often view security as a compliance requirement. They know they have to comply with standards such as PCI, ISO, or HIPAA, so they do. If the company can pass an audit, that's all that matters.

   Disconnect: Compliance standards may address all the risks a certain business has – but they may not. Relying on an outside standard really means a company is not taking responsibility for their own security.

The reason most businesses aren't where they want to be when it comes to cyber security has to do with their *culture*, *perspective*, and *strategy*.

Companies need to seek better connections between their IT and non-IT executives – and the responsibility to help form those connections goes both ways.

On the one side, IT personnel must become better at "business speak." That means discussing security in terms of:

- **Business processes.** Where do vulnerabilities exist and how do we address them?
- **Business value.** What do security measures do to protect the assets and interests of the business?
- **Business progress.** How do security measures actually advance the strategic goals of the business?
- **Business risk.** What is the financial downside of not implementing the proper security measures?

Remember, as a general rule of thumb, the moment IT people start speaking "jargon," their non-IT audience will tune out!

On the other side, non-IT executives and boards of directors must step up and offer their full buy-in. That includes acknowledging the key role cyber security plays in the business, engaging in productive dialogue with IT, championing security initiatives, and arranging for appropriate funding. The key differentiator in successful security programs is the involvement of executive leadership.

Perspective:

Recognizing that Security is a Marathon

When a company has a disconnect in their culture, they tend to also have a faulty security perspective. Namely, non-IT executives don't recognize that security is a marathon – and one that has no finish line.

For example, say a company has all the people and tools setup to ensure reliable security for their business. There is still the daily grind of security that has to take place: the new wave of Oracle patches that have to be implemented, the millions of lines of logs that have to be reviewed, the service providers whose activities and transactions must be monitored.

Then there are the regular security tests that have to be performed, including penetration tests that may reveal new vulnerabilities. Hackers keep developing more sophisticated techniques, so new software and solutions may need to be purchased and implemented.

Security can never be "put to bed." It is never finished. Cyber security will always be on the agenda at board meetings because security is a journey that requires headcount, budget, governance, executive-level decisions, continuous improvement, and all the rest of it… just like any other key area of the business.

Strategy:

Getting Serious about Security

Understandably, if a business has disconnects in their culture and perspective when it comes to security, they will not have a good cyber security strategy in place, either. This may appear as:

- **A reliance on compliance.** As noted previously, the entire security strategy of a company might be "whatever the regulations require."
- **A reaction to an action.** If an audit reveals a vulnerability or a headline screams about a new cyberattack, a company may scramble to fix a problem without adequately weighing the real risk, evaluating alternatives, and choosing the best approach.
- **An abdication of an obligation.** Non-IT executives may pass the buck, making this a pure IT problem, rather than looking at cyber security like any other business risk area.

Consider an example. Suppose a company is audited, and the auditor comes back and says, "You have to buy an IDS." In the absence of a sound cyber security strategy, there's no high-level business discussion. No dialogue about options. It's a fire drill: "Buy an IDS as fast as possible to plug the hole." Which IDS? *Any* IDS!

Such a reactionary approach, while comical, is actually a common occurrence. It can result in the purchase of a tool with too many or too few capabilities compared to the needs of the business, the expenditure of unnecessary costs, and a negative impact on affected business processes.

Security can never be "put to bed." It is never finished. Cyber security will always be on the agenda at board meetings because security is a journey that requires headcount, budget, governance, executive-level decisions, continuous improvement, and all the rest of it… just like any other key area of the business.

A cyber security strategy with appropriate governance procedures would put the brakes on such a hasty action. Business and IT personnel would sit at the table and discuss such questions as:

- What is the nature of the risk that the audit revealed?
- What are we technically required to do to comply with regulations?
- Will this tool adequately address the risk for our business, or do we need additional security precautions as well?
- What kind of tool do we select? What capabilities are critical and which are optional?
- Does it make sense to purchase this tool and add it to our existing security matrix?
- Should we consider a broader solution that includes this functionality plus other security measures, and use that to replace and augment our current security environment?
- Is this tool something we want to handle in-house, or outsource?
- How will the tool integrate with our current business processes?
- How will the tool impact interactions with our customers and our vendors?
- What is the best long-term security solution, taking into account the growth and goals of our business?

The result will still likely be a tool implementation, but it will be wrapped in a solution that is known to be best for the entire business, present and future.

Getting Where You Want to Be When It Comes to Cyber Security

Where do you begin if you don't have the best foundation of culture, perspective, and strategy for good cyber security? A poor approach is to try to plug leaks haphazardly. Instead, the first step is to perform a baseline assessment to identify where your company is from a technical and maturity standpoint. Such an assessment will analyze your business objectives and security risks, current security tools and practices, executive involvement, incident response preparation, governance policies, organizational structure, reporting, and more. The results can then be translated into a strategic roadmap to mitigate problem areas, establish a solid security profile, and set up a framework for continuous improvement.

You can perform a baseline security assessment in-house, but it is often preferable to draw in an objective third party. A cyber security provider can provide an unbiased analysis and help structure a strategic roadmap based on their experience of working with hundreds of companies.

Achieving security for your company is not an impossible dream. You can get where you want to be when it comes to cyber security by creating a culture, perspective, and strategy that upholds security as a mission-critical component of doing business well.

Additional reading

Consulting Services

Matthew Goche is a Vice President in Sungard AS' consulting business responsible for security services.

He leads the development of Sungard AS' security solutions and expansion into new client markets. Mr. Goche firmly believes that his role includes educating organizations on the risks to their business, brand, data, employees, and customers posed by security vulnerabilities.

He can be contacted at matthew.goche@sungardas.com

About Sungard Availability Services
Sungard Availability Services is a leading provider of critical production and recovery services to global enterprise companies. Sungard AS partners with customers across the globe to understand their business needs and provide production and recovery services tailored to help them achieve their desired business outcomes. To learn more, visit www.sungardas.com or call 1-888-270-3657.

Trademark information
Sungard Availability Services is a trademark or registered trademark of SunGard Data Systems or its affiliate, used under license. The Sungard Availability Services logo by itself is a trademark or registered trademark of Sungard Availability Services Capital, Inc. or its affiliate. All other trademarks used herein are the property of their respective owners.

Connect with Us