CSO
Custom Solutions Group

SECURITY LEADERSHIP SERIES:

Security Strategies for Success

Are you protecting the information that matters most?

CITRIX®

TABLE OF CONTENTS

CSO
Custom Solutions Group

CITRIX®

INTRODUCTION

SECURITY HAS NEVER BEEN SO CHALLENGING. Trends such as mobility, bring-your-own device and cloud computing mean that more people are accessing sensitive business information from more places and in more ways than ever before.

For IT, the challenge is to protect this information from loss, theft and increasingly sophisticated threats while addressing privacy, compliance and risk management mandates. Solid security strategies must include smart policies, rigorous enforcement and deep monitoring/reporting, as well as provide people with the level of access to business resources that they need to get their work done.

Citrix, a recognized leader for its contributions to the advancement of information security, can help you take a "protect what matters" approach to security and risk management that's right for your organization. Citrix gives business powerful ways to address key security and compliance priorities by ensuring the right level of secure access for every individual and situation. As business moves across locations, networks and devices, IT has the visibility and control it needs to protect and guard sensitive information assets without having to compromise workforce and end user mobility, freedom or productivity.

Complemented by industry-leading security partners, Citrix offers secure-by-design solutions to help you protect the information that matters most to your business.

In this exclusive Security Leadership Series eBook, Citrix chief information security officer Stan Black and chief security strategist Kurt Roemer share best practices for:

- Leading meaningful security discussions with the board of directors
- Engaging end users to protect business information
- Meeting security-related compliance requirements

For IT leaders, these security strategies for success are essential reading. Get started today. And don't forget to view and share the infographic: Are You Doing All You Can to Protect Your Critical Business Information?

4 SECRETS TO MEANINGFUL SECURITY DISCUSSIONS WITH THE BOARD OF DIRECTORS

Corporate boards are more interested in security than ever before. Here's how to engage them in a strategic dialogue about a topic with bottom-line implications.

"Security has evolved from a technical issue into a broader issue of intense business interest to corporate boards."

—KURT ROEMER
CHIEF SECURITY STRATEGIST
CITRIX

Security was once the exclusive province of IT departments. These days, with increasingly sophisticated threats proliferating across geographic boundaries, cloud computing, mobility, and everything "bring your own," security has finally won the ultimate badge of corporate honor: a seat at the board of directors.

"Security has evolved from a technical issue into a broader issue of intense business interest to corporate boards," says Kurt Roemer, chief security strategist at Citrix.

That heightened interest is hardly surprising given the seriousness of security-related risks, which include exposure of sensitive information, damage to your company's reputation, and—most important of all—serious harm to the bottom line. For IT leaders, the upshot is more frequent boardroom discussions about the core pillars of any solid security plan: policies, enforcement mechanisms, and monitoring/reporting. To lead those meetings successfully, follow these best practices:

1. Speak the language of the boardroom

Board members discuss business issues in business language rather than technical terms. Follow suit in board meetings by focusing on critical threats, the material risks they pose, the best options for mitigating them, and breach preparedness.

Be concise when discussing those topics, and avoid conjecture. Board members are interested strictly in facts. Use clear, easily understood charts and diagrams as well to illustrate important issues like your company's current security posture and future goals.

"That way you can show the board exactly where you are, where you're going, and how you'll get there," says Stan Black, chief information security officer at Citrix.

Be prepared for plenty of questions, too. Board members will want to know how your organization stacks up against peers in your industry, for instance. Crisp, informative, and

thoroughly researched answers will reassure them that your strategies are sound.

2. Explain the core elements of your risk mitigation efforts

Well-designed risk mitigation strategies are also reassuring. Such strategies should take a "protect what matters" approach to safeguarding your company's most important, vulnerable, and heavily regulated data. The board will want to know how you prioritized sensitive data, so describe the process you used. In addition, guide them through:

- Your policies for handling business information, in the cloud as well as on company-owned and personally owned devices both inside and outside the office
- How you enforce those policies and train employees to follow them
- How you prevent the loss of essential data

In particular, make certain board members understand that persons like themselves with access to an organization's most sensitive information are high-value targets who must be especially diligent about following security policies. Be sure to update the board about any changes in your company's governance obligations too, as well as the steps you're taking in response.

Of course, new and emerging threats pose dangers no matter how good your mitigation strategy is, so deploy security technologies in layers that account for your network and your users, as well as their apps, data, and storage.

3. Describe your breach preparedness and incident response plan

Even the best security measures can fall prey to attacks, so show board members you're ready by explaining your incident response plan, including who's on the response team, who's authorized to mobilize it, and under what conditions. Describe your internal and external communication plan as well, and discuss your disclosure triggers for security incidents. Some disclosure thresholds are defined by law, but others rely on discretion, and board members should provide direction on how descriptive they need to be.

Should a breach occur, brief the board promptly about what happened, the potential impact on your company and your customers, how long it will take you to fix the problem, and what you're doing to prevent repeat occurrences. Provide regular updates too, and set a clear schedule for when board members can expect your next report.

4. Use meaningful security metrics to measure success

Most boards wish to monitor security readiness on an ongoing basis. A security dashboard will provide them quick access to the most relevant information.

"The dashboard provides context to security risks and enables the board to oversee the reduction in critical exposures," Black says.

Use metrics that are easy for board members to understand and relevant to their concerns, such as threats identified, time to response, end-user devices lost, and audit results. In addition, revisit your metrics periodically, adapt them to your company's evolving threat landscape, and inform the board about any major changes to your architecture, technologies, and strategy.

Presenting to the board of directors may be a new experience for some in IT, but it doesn't have to be a difficult one. With the help of the guidelines above, board meetings can be an opportunity to engage your company's most senior leaders in a strategic dialogue not only about security, but about mobility, cloud computing, and the evolution of the workplace. ■

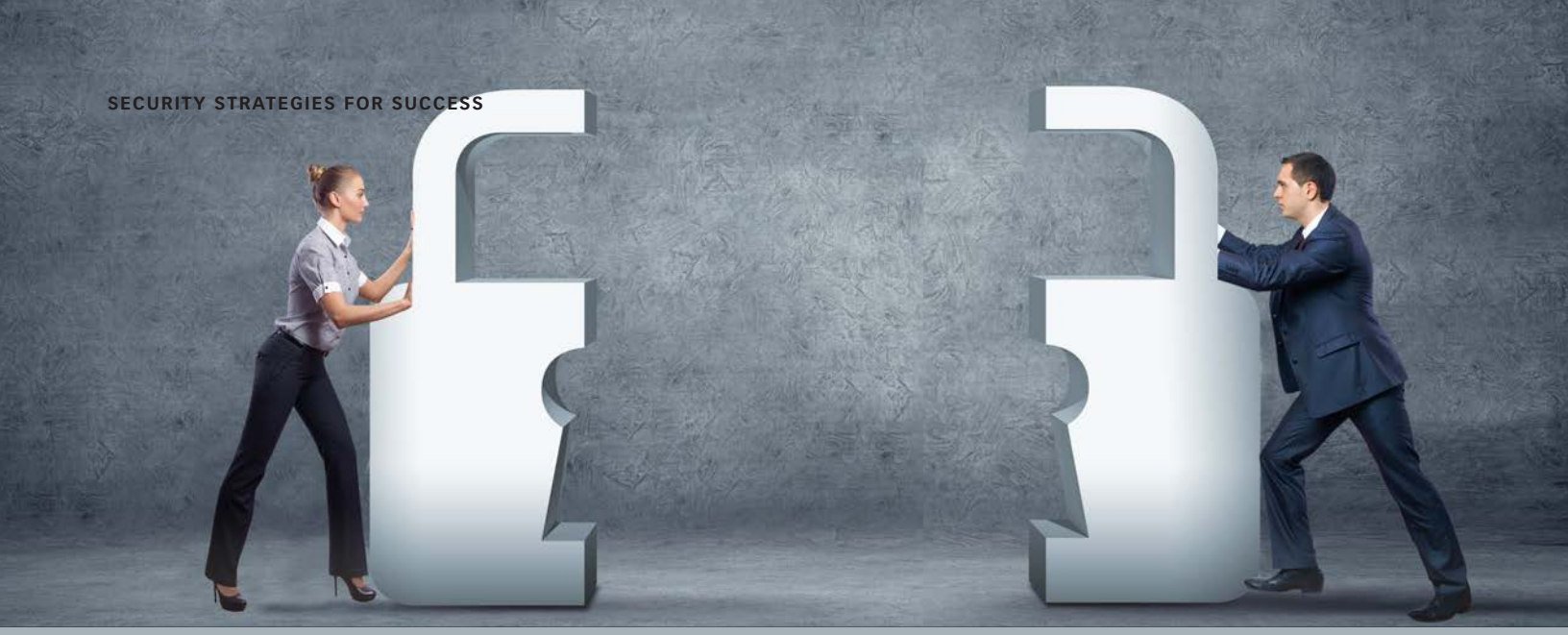
HOW CITRIX CAN HELP

Security is of greater interest to corporate boards than ever before, and technology plays a central part in any effective security strategy. Citrix ensures security and compliance for critical business information while empowering your workforce to work anywhere, anytime, on any device.

Citrix XenDesktop allows companies to publish Windows apps and desktops in the data center, where IT can maintain centralized data protection, compliance, access control, and user administration. Citrix XenMobile provides rich enterprise mobility management capabilities, including identity-based provisioning and control of apps, data, and devices. Citrix ShareFile enables employees to share data securely with anyone and sync data across all of their devices. Citrix NetScaler adds a unified management framework that lets IT secure, control, and optimize access to apps, desktops, and services on any device.

Citrix solutions are "secure by design" systems carefully architected to minimize vulnerabilities and are complemented by state-of-the-art offerings from industry-leading security partners. The end result is a comprehensive platform for protecting information that gives security-conscious board members lasting peace of mind.

To find out more, please visit www.citrix.com/secure



5 BEST PRACTICES TO MAKE SECURITY EVERYONE'S BUSINESS

Employees are one of your greatest risks to information security. Use these five proven techniques to strengthen your security strategy and protect your business.

"When policies are developed collaboratively across the company, and security awareness is woven into the culture, violations are infrequent."

— STAN BLACK
CHIEF INFORMATION SECURITY OFFICER
CITRIX

Menaced by an ever-expanding array of increasingly potent threats, today's highly mobile employees are front-line participants in the struggle to secure the enterprise. So while solid security strategies must include smart policies, rigorous enforcement, and deep monitoring/reporting, they must also reflect the needs and habits of the company's users.

"End users are ultimately where security succeeds or fails," says Kurt Roemer, chief security strategist at Citrix.

Unfortunately, keeping employees both safe and satisfied isn't easy. Employees want anywhere, anytime access to information from any device without cumbersome security protections slowing them down. Business managers want to safeguard important information without inhibiting growth, innovation, and competitiveness. IT departments want to keep everyone productive while recognizing that employees and their devices are often the weak links in the security chain.

To balance those competing interests, security leaders should follow these best practices:

1. Educate users

An informed, security-conscious workforce is every company's first line of defense against security threats, so teaching people how to work safely from any location on any device must be a top priority.

Simply preaching best practices is a recipe for failure. Take the time to understand who your users are, what they do, and what they need. Then explain your company's security policies to them in terms that are easily understood and relevant to their role.

"Relevance is key," Roemer says. "Everything you present should be specific to a person's function rather than one-size-fits-all."

It should also be personal, Stan Black, chief information security officer at Citrix adds. For example, in addition to work-related security training, Citrix gives its employees advice on topics like securing a home wireless network and helping their kids use the Internet safely.

"We try to tie all our education efforts to the full lifecycle of

security, not just what people do at the office," Black says. That makes security training more valuable for employees while also protecting sensitive data from poorly secured personal hardware.

2. Engage with line-of-business organizations

Close working relationships between IT executives and line-of-business managers are an essential ingredient for effective security. Meeting regularly with business decision makers empowers security leaders to build appropriate safeguards into new business initiatives right from the beginning. It also gives them an indispensable, up-close perspective on a business group's unique risks and requirements.

"You'll learn more about operational processes and potential dangers that you'd never know about otherwise," Black says. "You can then incorporate those insights into your security plans and make them even richer."

3. Take a modern and mobile look at security policies

As critical as it is, training alone doesn't ensure strong security. Many of the devices, networks, and storage systems employees rely on these days are outside of IT control.

"IT needs to update traditional security policies for the new mobile and cloud services reality," Roemer observes.

Start by thinking through how strictly you want to limit access to your company's data based on where an employee is located and what kind of device they're using. Most companies adopt graduated policies that protect sensitive information more carefully than public information and provide less access from consumer-grade and "bring your own devices" (BYOD) than from more thoroughly "locked down" enterprise-grade devices.

Then revise your security policies to reflect risks like storing business data on personally owned devices, posting passwords on a computer monitor, or using a USB storage device you found on the floor.

4. Enforce policies fairly and consistently

Security policies can lose value over time if users don't believe violating them has consequences—or worse yet, if they believe bypassing them improves productivity. Policies must be maintained and kept current with the business. Security leaders must therefore enforce policies fairly and consistently.

"When policies are developed collaboratively across the company, and security awareness is woven into the culture, violations are infrequent," Black says.

5. Automate security seamlessly

To further reduce policy violations, use security software to automate policy enforcement. For example, many security solutions can implement desired behaviors—like encrypting business data on mobile devices—by default. They can also build tighter security into core elements of the user experience by automatically preventing employees from running unauthorized apps over the company network or limiting which apps people can open email attachments with, for example. Other solutions provide logging and reporting functionality that can help you prove to auditors that you've applied appropriate policies scrupulously.

Even so, software is ultimately just one piece of the security puzzle.

"To really protect the company you have to get to know your line-of-business groups and your end users," Roemer says.

Ultimately, the best security strategies are as much about people as technology. ■

3 STRATEGIES TO MANAGE COMPLIANCE MANDATES

Meeting security-related compliance requirements is an increasingly complex job. Focus on these three strategies to easily manage compliance.

"Most companies have between three and five different types of data classifications, ranging from public to top secret."

— STAN BLACK
CHIEF INFORMATION SECURITY OFFICER
CITRIX

Here's good news for security leaders: If you've established sound policies, enforce them rigorously, and thoroughly monitor and report security effectiveness, you're well on your way to protecting your company from today's growing swarm of increasingly potent threats. Now here's the bad news: More and more auditors, regulators, partners, and customers are demanding defensible proof of that fact.

"Globally, there are over 300 security and privacy-related standards, regulations, and laws with over 3,500 specific controls, with more coming all the time," says Stan Black, chief information security officer at Citrix. "The people responsible for those rules want evidence that you're in compliance."

The consequences for disappointing auditors and regulators can be severe. Failure to comply with today's ever-expanding thicket of security-related compliance requirements can result in fines and penalties, outraged customers, loss of sensitive data, increased scrutiny from regulators, and costly damage to your organization's brand and reputation.

Not surprisingly, then, compliance has become a topic of intense interest to senior executives and board members. To bolster their confidence that your company meets all of its requirements—and can defensively prove it—follow these best practices:

1. Enable access while protecting information

Adopting a comprehensive approach to identity and access management, combined with an intense focus on sensitive data and relevant reporting and metrics is an important balance. Policies should specify granular data access privileges based on where employees are located, what network they're on, and which device they're using, with additional controls commensurate with risk. For example, access should be further scrutinized when utilizing a personally owned smartphone over a public network, than when using a company-owned laptop at the office.

Job role is another important variable. "You should grant access only to people who have a need to know for their role and function," advises Kurt Roemer, chief security strategist at Citrix. Role-specific training and automated role-based access control will ensure employees understand your policies and follow them.

You should also diligently enforce your policies with the

help of a robust security architecture. For example, data-focused security measures help protect data "in transit" across public and private networks, "at rest" in cloud-based or on-site storage, and "in use" on end-user devices. It also manages device security and other assets employees use to access information, builds tighter security controls into the company's applications and networks, and manages those controls both centrally and when management responsibilities are distributed.

2. Control sensitive data

Most security mandates apply chiefly to personally identifiable information, healthcare records, payment transactions, and other classified data. To comply with mandates, you must first identify sensitive data by creating a classification model for the various kinds of information your company creates, transmits, and stores.

"Most companies have between three and five different types of data classifications, ranging from public to top secret," Black says.

Next, make data classification assignments and prioritizations. To ensure the right data ends up in the right categories, involve a wide cross-section of stakeholders in this process, including representatives from your business groups, legal department, and operational functions.

Now you're ready to implement policies and enforcement mechanisms for securing data based on how sensitive it is, where it's stored, and where it's being accessed. For example, you might choose to control public data minimally regardless of user, network, and device, but limit access to confidential information on "bring your own" and consumer hardware. Always apply your strictest controls to your most sensitive data. "It makes sense to deny access to sensitive data altogether on devices and networks that can't be verified as appropriately secured," Roemer says.

Once again, security solutions can help you enforce classification-based policies automatically.

3. Audit, measure, and demonstrate compliance

Comprehensive security reporting is always important, but especially critical when it comes to compliance. "Auditors and others want to see clear evidence that you did what you said you would," Black says.

Satisfying those demands takes systematic logging, reporting, and auditing processes thorough enough to track when specific users access specific apps and data, and flexible enough to address new regulations and standards as they emerge. Create a reporting dashboard as well where authorized managers can see the latest compliance goals and results. "Otherwise you'll be pushing around spreadsheets that are out of date before anyone even gets them," Black notes.

Should an audit uncover gaps in your compliance measures, take a cradle-to-grave approach to resolving them by centrally tracking issues from detection to closure. Treat the people who found those issues as colleagues rather than adversaries. Internal auditors can help you eliminate risks and justify additional security investments. External auditors can provide valuable, unbiased feedback on your compliance regime.

Consulting with peers is often similarly helpful. Executives in your field may be reluctant to speak freely, but security leaders in other industries are often willing to exchange useful insights if everyone commits to nondisclosure agreements in advance.

Opportunities like this make clear that, for all its difficulties, compliance can pay real dividends. "Quite honestly, the reason most of these laws and standards exist is because businesses have struggled to understand and deliver a 'best practice,'" Black says.

Meeting today's constantly shifting compliance requirements is an excellent way to test your defenses regularly and keep them aligned with the business need for security. ■

EMBRACE MOBILITY SECURELY WITH CITRIX

IT has to maintain compliance and protect sensitive information wherever and however it's used and stored — even when business and personal apps live side-by-side on the same mobile device. Developing a truly comprehensive and security-conscious mobility strategy is now a top priority for every organization.

To protect what matters most for your organization, choose mobility management and app delivery models that make the most sense for your business and your mobile use cases. Also collaborate with users to develop a mobility strategy so you can better meet their needs while gaining a valuable opportunity to set expectations, automate outcomes, be clear about ownership, and make sure that people understand IT's own requirements to ensure compliance.

Citrix provides a complete solution to enable secure enterprise mobility with a simple, convenient user experience your workforce demands. Incorporating complete technologies for MDM, MAM, containerization, application and desktop virtualization, and networking, the end-to-end solution allows ample flexibility to support your organization's secure mobility requirements.

To find out more, please visit www.citrix.com/secure

INFOGRAPHIC

CLICK HERE TO VIEW THE FULL GRAPHIC