LogRhythm®

The Security First Guidebook:

Learn How to Create a Security-First Culture in Your Organization

Contents

Learn How to Create a Security-First Culture in Your Organization

In 2020, you handled a global pandemic, a rapid shift to remote work, and the SolarWinds[1] supply chain attack. All of this opened a window into security operations—giving you the opportunity to discuss heightened security risks to your organization and the need for a security-first culture with your board.

With the events of last year putting a greater focus on security, pushing for more security visibility and increased budgetary support has become essential.[2]

By building a security-first culture, your company will experience[3]:

- Fewer malware intrusions
- Decreased likelihood of ransomware infections
- Reduced strain on the security team
- Increased trust from business partners and customers

This guide is full of key considerations, tips, and practical steps you can take today to build a security-first culture in your organization, along with key takeaways to bear in mind for the future.

[1] Cybersecurity spending to increase following SolarWinds hacking, January, 2021
[2] IBID
[3] Security Awareness Training as a Key Element in Changing the Security Culture, September, 2020

What Does it Take to Create a Security-First Mindset?

To create a security-first mindset, you need a vision for what this security-first mindset looks like company-wide and a strategy on how to get there.

That vision is the ideal state of security-first your organization needs to achieve — everyone is trained, aware, and instinctively acting in a security-first manner.

"Strategic visions become real only when the vision statement is imprinted in the minds of organizational members and then translated into hard objectives and realities."[4]

Are you ready to shift your organization's mindset?

[4] Thompson, A. A., Strickland, A. J., Gamble, J., and Thompson, A. A. (2005). *Crafting and executing strategy: The quest for competitive advantage: concepts and cases.* New York, N.Y.: McGraw-Hill/Irwin. Sixteenth Edition, p 26

Shifting the Security Mindset from Protection to Asset Generation

Establishing, communicating, and getting organizational support along with funding for your team's goals can be challenging. This requires building advocates across the company, and possibly even speaking to the board of directors (BOD). You need to come up with the right strategy for that advocacy along with a possible security presentation to the BOD.

This guide and accompanying presentation template will put you in control of the practical steps to building a winning security awareness program at your organization. These tools provide a method to demonstrate the value that a security-first mindset can mean for positive brand recognition and continued revenue generation.

Armed with a security-first mindset, your security-aware employees will turn your security awareness program into a cultural asset that will reduce organizational risk.

Download the LogRhythm Security First Presentation Template

Establishing Your Security Awareness Program

Strategic Security Training Considerations

To adequately protect your organization, you must create a security-first mantra within your organization, moving from a "command and control" IT group-only mindset to a company-wide collaborative security-first effort.

To be that agent of change in your organization, to elevate and embed a security-first mindset into the culture of your company, you'll need to learn how to:

- Build advocates about shifting the company mindset from protection to cultural asset
- Show consumption and ROI of your program to quantify security awareness for funding
- Create effective security awareness training programs
- Develop a strategy to promote security awareness throughout the entire ecosystem
- Continuously reinforce the importance of a security-first culture
- Plan for future trends and challenges

Turning Your Security-First Program into a Cultural Asset

To adequately protect your brand, enable continuous business operations, and reduce risk, you need to elevate security out of IT and into the mindset of the entire company.

As the leader of the security team, the goal has remained the same: protect your organization and keep customer, employee, and company data safe. Current cybersecurity statistics show that 94% of malware is delivered via email and 80% of reported security incidents are attributed to phishing. You understand that success or failure of your security program depends as much on employees and processes as it does on the products used for protection.

Are you ready to shift your organization's mindset?

94%
of malware is delivered via email

80%
of reported security incidents are attributed to phishing

[5] Top cybersecurity facts, figures, and statistics, March, 2020
[6] Security is more than a process... It's a proficiency, December, 2019

The Vision

Turn a Security-First Mindset into a Company Asset

Your goal is to raise the security awareness of everyone, teaching how to make security a part of the everyday conversation when conducting day-to-day business such as:

- Choosing a technology vendor
- Working with supply chain partners
- Opening emails
- Opening doors
- Discussing remote work situations
- Independent contractor considerations

Your job isn't an easy one, but you've got the grit to take it on, and LogRhythm is here to help you with security awareness resources to guide the way.

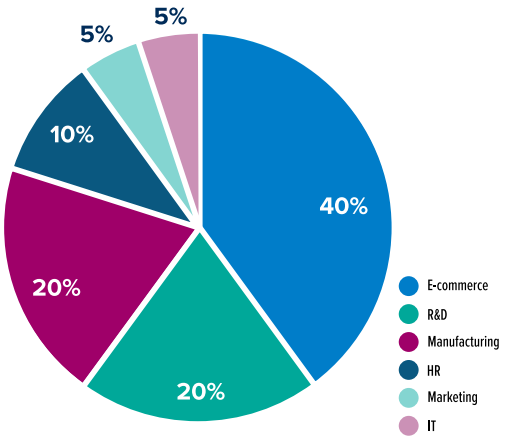
The Business Case

Develop Your Security-First Awareness Strategy

Employees are your first line of defense. It makes sense that they should be educated and made aware of the consistency and persistence of the security threats to your organization.

You need to develop a business case for security awareness and translate that into how a security-first awareness program will benefit the company overall. To build the business case, consider the users of the business systems and workflows in your organization that are the most vulnerable to threats to be consumers[7] of your team's security services.

With that in mind, create a pie chart that illustrates what percentage of your SOC services and budget are consumed or used by those business units.



With this chart, you can easily illustrate and point to where the most security resources are consumed.

[7] *How to Get Ecosystem Buy-in*, Harvard Business Review, March–April 2017 issue (pp.102–107)

Obtain Funding

Prepare to Meet with Your CFO and Board

You will need to meet with your chief financial officer (CFO) to present your security consumption chart, discuss how your security services are used by the entire company, and review how security services are currently being funded. Outline to your CFO budgetary items whose cost is shared across business units such as mandatory partner compliance and the cost of alignment with cybersecurity liability insurance.

Ask to see if any activity-based costing (ABC)[8] is available to assign the direct and indirect costs of providing security to the company. Work with your CFO to align your consumption chart with his ABC costing. If ABC costing isn't available, ask what percentage of revenue is allocated for security so that you can work to align your budget and services with that budgetary expectation.

All of this will help you establish a basis in fact for security funding and budgeting moving forward, in addition to building the blocks to establish security as a company-wide service being consumed. And those business units should pay for their consumption.

Your ability to translate the security services you provide into financial terms and illustrate security services consumed and value delivered is paramount to obtaining the funding you need.

"If my CISO were exploring a new security investment, I would want to understand the specific risk we are trying to mitigate, the effectiveness of that solution, and their annual cost."

Barry Capoot, CFO, LogRhythm

[8] What is Activity-Based Costing (ABC)?, February, 2020

Security Operations Maturity

What used to be in the background has now been pushed to the forefront as consumers, clients, and partners must verify that doing business with you falls within their security parameters. Simply tracking phishing attempts or malware found is not enough anymore.

Assessing your organization's security maturity level using the LogRhythm Security Operations Maturity Model (SOMM) will give you a security operations benchmark that you can use to compare with similar organizations in addition to providing an internal roadmap for moving your security operations up the maturity ladder. Complete the SOMM self-assessment here and work to create strategies that will move the company up a level or two in its security management practices by conducting a gap analysis. The resulting gap analysis will:

- Show where your organization ranks in the security maturity model
- Describe how/why security is aligned with the organization's business model
- Diagnose the current state of security-first behaviors with respect to the norms of the company
- Assess the organization's tolerance to making security changes
- Identify change enablers and barriers

Once you know where you stand with regards to your security operations maturity, it's time to check in and see where your security operations stand regarding the alignment information technology (IT) has with the entire organization.

That IT governance falls to the chief information officer (CIO), whom you most likely already meet with. Work with your CIO to establish that security awareness is integrated into their IT Strategic Alignment Maturity Model[9] to ensure commitment and support for your security-first program.

[9] Luftman, Jerry N, et al; (2004). *Managing the information technology resource: Leadership in the information age.* Upper Saddle River, N.J.: Pearson Education. Pg 69-73

Using Security Maturity and Metric Measurements

Measure What Matters

The LogRhythm SIEM dashboards and reports provide many ways for you to monitor, measure, and communicate the state of your security capabilities, enabling you to easily outline your current security capabilities and track your gains. Embedded security operation center (SOC) metrics enable you to focus on continuous reduction of mean time to detect (MTTD) and decrease the mean time to respond (MTTR) to threats. With these reports, you can illustrate your security operation successes and how those successes benefit the company in terms of reduced risk.

You can also present on your SOC team's operational effectiveness over time by tracking these KPI and SLA-oriented security metrics: Alarm Time to Triage (TTT), Alarm Time to Quantify (TTQ), Time to Mitigate (TTM), Time to Recover (TTR), Time to Respond (TTR).

Use these metrics to tell a story of the threats the SOC has stopped and the risk reduction benefit to the business. With these metrics, you can see what is working and what isn't and make adjustments to technologies used and your security-first awareness training, contributing to reduced risk to the company.

These metrics will not speak to everyone at a board level. You will need to translate the progress of the Security First program into business value to show the impact to the bottom line

Presenting to the Board

Once you have the SOC consumption chain[9] identified, know where your organization ranks on the SOMM, and have established your baseline metrics, you will have the beginnings of a fact-based road map. Use your roadmap to build a presentation on security investments the BOD needs to consider investing in your program.

> **"It cannot be emphasized too strongly that the sponsorship of a senior executive is essential to the successful formation of IT strategy."[10]**

You need to build advocates. Ask to be invited to the next BOD meeting to identify who on the board might be an advocate for your programs. In your presentation, make security ROI tangible. Here are some presentation ideas for you:

- Create slides about specific security events and explain what it saved the company in terms of brand reputation, loss of revenue, etc. Discuss the depth of some of the breaches along with the sensitivity and value of the information accessed.
- If a recent hack has made the news like SolarWinds or the Jones Day[10] law firm data breach, investigate it and create a breach slide, explaining why the measures you have taken mean that type of security incident won't happen in their house.
- Quantify the reduction of risk in terms of ROI. For example: If we make this PCI e-commerce security investment, it will reduce our risk by 50 percent, enabling our sales team to get new contracts. Explain how the real return can be seen in the reduction of the likelihood of a data breach.
- With the information you have gotten by working with your CFO, create a consumption slide including ABC costing and revenue information. When you present your budget, show that you understand where the company's revenue comes from, what percentage of that is spent on security, and whom all are consuming it.
- Present on where you would like to take security measures/awareness training further, what symbolic and substantive acts the company can do to reinforce security awareness, and what it will do for the company when you do (keep company safe, build trust, enhance brand reputation, build a competitive advantage).

Work to get the board to support a "Be Security First" program that raises awareness and embeds security into the cultural norm of the company by telling stories. Use real-world, relatable examples, and speak in the BOD's language by showing the business value and not being too bogged down into the technical details.

[10] Luftman, Jerry N, et al; (2004). *Managing the information technology resource: Leadership in the information age.* Upper Saddle River, N.J.: Pearson Education. Pg 40

Creating Effective Security Awareness Training Programs

When it comes to security awareness, you are challenging cultural norms at every turn. By embedding security-first thinking into the company's mindset, behaviors will change, creating the opportunity for a sustainable reduction in risk for the company.

According to a recent Forrester report on managing the human risk in cybersecurity[11] "only 27 percent of global information workers say they are aware of their current security policies, and eight percent of them admit to ignoring or going around their security policies." As CISO, you need to work to create an understanding within the company regarding how security impacts and influences business and how security is aligned with business goals. Management teams must understand that being security-first is a goal that not only protects the company but also strengthens and improves the culture around it.

> **"If you try to fight an organization's culture, you're just going to be pushing a rock uphill. Having advocates can help—because then you won't be fighting against the culture as much. Instead, you could be helping to drive the culture."**
>
> **James Carder, CSO and VP of Labs at LogRhythm**

Create a cross-functional security-first team consisting of the leaders of the identified security consumption teams. Meet on a regular basis to illustrate what security precautions have been taken by the company, help identify gaps, goals to close those gaps, define initiatives to address those gaps, and measure the results. Find out who handles internal communications at your organization and get their buy in to promote security as they are communicating other business matters.

[11] How To Manage The Human Risk In Cybersecurity, January, 2021

Building Advocates

As your team meets with these business units and discovers their unique security needs, demonstrate your value to them by reviewing the SOC services they use and how you and your team protect them every day. Remind them that all employees must be stewards of a security-first mindset. Have those leaders invite you into their domain to present on security to build awareness and learn what security differentiators and needs each business unit may have. As you build that awareness, a security-first mindset will begin to emerge, new processes are established, and you can begin to measure the success of the program.

To get security right, you must have the right cross-functional team in place, working to actively embed a security-first mindset into the culture of the company.

Security Awareness Meeting Discovery Tips

Find out what vendors each business unit relies on to conduct their business and audit their security, asking question such as:

- Is the e-commerce PCI compliant?
- How secure is your marketing department's email vendor?
- Can you be certain your customer and prospect email lists won't be stolen?
- How secure is the customer service department's CRM system?
- How many of their cloud-based applications have a modern web-based front-end UI with a back end that was written in non-memory-safe code back in the 1980s and 1990s?

Include them in reviewing new vendor contracts for security, so they can understand how security requirements are a part of the picture.

Identify which partnerships you may need to build within your company to gain support for your security first program.

Reinforcing Your Security Awareness Program

Hiring the Right Security-First Team

Your hiring strategy will provide a documented plan for your security operation and will help you execute on the vision you have for your organization.

> **"Your hiring strategy should serve as your blueprint. If you choose to do so, sharing a hiring strategy with a prospective employee can also show a candidate that you're thoughtful in building your operation and give them a level of confidence in your leadership abilities."**
> **James Carder, CSO and VP of Labs at LogRhythm**

Documenting your staffing strategy will help you to identify where you have gaps and areas for growth and improvement. People who are open and willing to share information, encourages interoperability, which in turn leads to the ability to act with agility. Part of reducing the risk of a breach is having essential roles and highly skilled people as part of your security operations. And when those people are armed with the right tool such as the LogRhythm SIEM Platform, companies can move from making well-intentioned, hastily formed actions to sophisticated, automated responses.

Staffing models include in-house, outsourced consultants, or a hybrid of the two. Regardless of model, it's helpful to have a diverse group of individuals on your team whose skills go beyond security. An understanding of business, cross-functional areas, and people skills can all be critical skills when building your security awareness team. Your ideal team would include a mix of C-level and mid-level management, engineer, hands-on responder, and business analysts who know the business cross-functional workflows. All should have one thing in common: commitment to a security-first culture.

Start building your team with our **SOC Job Description Templates**

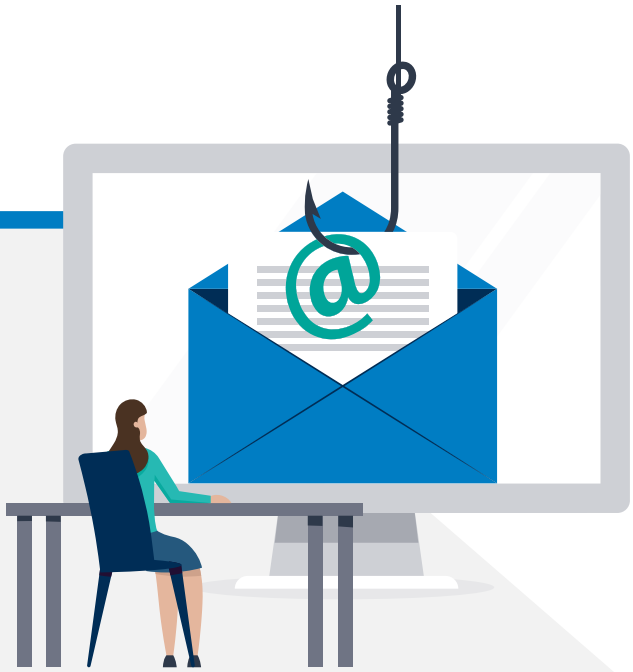
Promoting and Reinforcing Security Awareness Throughout the Ecosystem

Symbolic and Substantive Actions

It's been proven that a combination of symbolic and substantive actions[12] will have the greater impact on persuading stakeholders. Identify symbolic and substantive management actions that will support your security awareness program to get budgetary approval.

Symbolic actions might include items such as a security-first program announcement, posters, or T-shirts. Substantive actions could be awards for improving security KPIs and SLAs perhaps with a "Security Employee of the Month" award or creation of a security Slack channel[13] to encourage employee conversations about security concerns they encounter, such as phishing emails.

Phishing education is a large part of a security-first employee training. You might create a phishing contest whereas part of the training, unknown to them, the trainees are sent a variety of phishing emails that are unexpected, sent outside of normal business hours, with unrecognizable email addresses, links to spoof Covid sites or Starbucks gift cards, and funky looking attachments. Recognize reported phishing emails.



[12] Berrone, Pascual and Gelabert, Liliana and Fosfuri, Andrea, The Impact of Symbolic and Substantive Actions on Environmental Legitimacy (January 1, 2009). IESE Business School Working Paper No. 778, Available at SSRN: here or here.

[13] Healthy security cultures eat lots of phish, May, 2017

Future Outlook

Driving organizational change is challenging, especially for areas that may have been viewed as cost centers in the past. You know that you need to ensure security is a top priority and that you need to have a plan to address elevating a security-first mindset. Below are key areas to keep in your sights:

Remote Workforce Security Awareness

According to a recent Fortune Magazine Analytics survey[14], 42 percent of office workers would prefer a hybrid model of in-office and remote work. Once the pandemic has calmed, there will be a continuing need to monitor and secure your remote workforce.

You will continue to need to get visibility into application workflows and usage, Office 365 activities, alerts on unexpected zoom attendees or sign-ons as endpoints and collaboration tools are monitored.

Internet of Things (IoT) Security Awareness

IoT technologies are a growing portion of the connected device landscape. By 2021, Gartner estimates that 25 billion IoT devices will be in service[15]. You will need to secure an increasingly wide range of devices, including autonomous robots[16] equipped with a variety of information-gathering sensors, and AI-driven HVAC systems[17]. Today's broader network includes securing and monitoring traditional desktop computers, tablets, IoT devices including AI-driven robots. Yet, according to a recent report by Palo Alto Networks[18], 98 percent of all IoT device traffic is unencrypted, potentially exposing sensitive data on the network to attackers.

[14] Remote, in-person, or hybrid work: What do people want?, March, 2021
[15] Gartner Identifies Top [10] Strategic IoT Technologies and Trends, November, 2018
[16] What are autonomous robots?
[17] [75]F, an AI-powered HVAC management startup, nabs $[4.75]M, March, 2021
[18] 2020 Unit 42 IoT Threat Report, March, 2020

Ready to Get Started?

With this guide, you have the building blocks for what information you need to present to key decision makers to reach your vision of the ideal security-first state your organization — everyone trained, aware, and instinctively acting in a security-first manner.

To adequately protect your brand, enable continuous business operations, and reduce risk, you must elevate security out of IT and into the mindset of the entire company.

When you do, your organization will experience fewer malware intrusions, decrease the likelihood of ransomware, reduce strain on the SOC team, and increase business trust across the board.

A world leader in NextGen SIEM, LogRhythm is your partner in protecting your organization, employees, and customers from the latest cyberthreats. Schedule a demo to learn how LogRhythm can help strengthen your organization's security posture. logrhythm.com/demo

Download the LogRhythm Security First Presentation Template

Be Security First

About LogRhythm

LogRhythm's award-winning NextGen SIEM Platform makes the world safer by protecting organizations, employees, and customers from the latest cyberthreats. It does this by providing a comprehensive platform with the latest security functionality, including security analytics; network detection and response (NDR); user and entity behavior analytics (UEBA); and security orchestration, automation, and response (SOAR).

Learn how LogRhythm empowers companies to be security first at logrhythm.com.

LogRhythm®

1.866.384.0713 // info@logrhythm.com // 4780 Pearl East Circle, Boulder CO, 80301