Criteria for Proactive Security

Business Drivers for Proactive Security

graylog

Table of Contents

03 Introduction

04 Investing in Incident Response

05 Regulatory Compliance

07 End of License

08 New to the Organization

10 Budget Cycle

11 Mergers and Acquisitions (M&A)

12 Strategic Initiatives

13 Graylog: The Security Solutions

13 About Graylog

Introduction

You're not satisfied right now with your current security processes. You think you need something, but you're not sure. Your budget might be tight. Your team might be small. You have a collection of tools that capture data, but they don't give you the insight you need.

Risk is a business constant, something that you'll never be able to eliminate. Instead of focusing on completely security risks entirely, you might consider asking yourself whether your IT security is mature enough to mitigate risks and resilient enough to respond to changes in the threat landscape.

At the same time, your security technology stack needs to align with your company's business goals. It's like Goldilocks dilemma. You don't want something too small because you might not be able to detect a security incident. You don't need something too big because it might be outside your budget or your team's experience.

You need something that's "just right."

What is that "just right" solution?

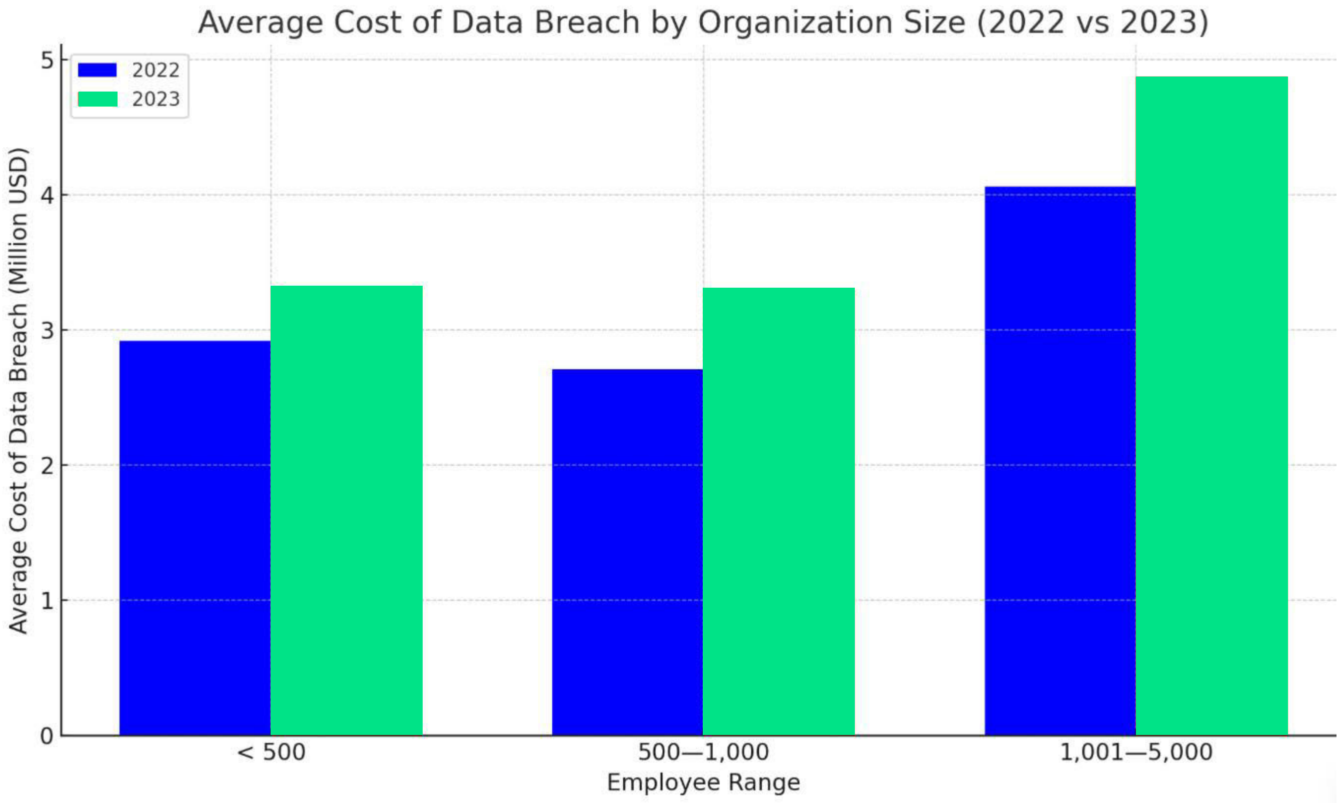
To answer that question, here are eight questions to consider:

1. Are you investing enough in IR (Incident response) given the rising costs of breaches?
2. Do you have regulatory compliance needs?
3. What is the current state of your software contracts/licenses?
4. Are you onboarding a new CISO or security team staff member?
5. What is your budget cycle?
6. Are your managed services providers giving you the value you expect?
7. Are you looking to grow with mergers and acquisitions?
8. Do you have strategic initiatives that require you to mature your security program?

Investing in Incident Response

Investing in a incident response plan in order to prepare and encourage your organization to think about the next steps in the immediate aftermath of a breach is an investment in with a verified return on investment. “In 2023, Organizations with high levels of IR planning and testing saved **$1.49 million** compared to those with lower levels,” according to the 2023 IBM Cost of a Breach Report. According to the 2023 IBM Cost of a Breach Report; “In 2023, organizations with more than 5,000 employees saw the average cost of a data breach decrease compared to 2022. In contrast, those with 5,000 or fewer employees saw considerable increases in the average cost of a data breach. Organizations with fewer than 500 employees reported that the average impact of a data breach increased by 13.4% from $2.92 million to $3.31 million. Those with **500—1,000 employees saw an increase of 21.4%**, from $2.71 million to $3.29 million. In the 1,001—5,000 employee range, the average cost of a data breach increased from $4.06 million to $4.87 million, rising nearly 20%.

Chart 1: 2022 vs 2023 costs of breaches by company size from 2023 IBM Cost of Breach Report”



Regulatory Compliance

Your business is growing. You want to move into new markets, but you need to uplevel your compliance. Yes, compliance is the word that most companies hate hearing because compliance comes with documentation.

All compliance is founded on the Big Three — Governance, Risk, and Compliance (GRC). To understand what you need to prove, let's start with the basic definitions:

- **Governance:** Giving leadership a way to make informed decisions
- **Risk:** Evaluating the potential impact and likelihood of a data breach
- **Compliance:** Documenting that established controls remain effective

If you're a smaller company with limited IT resources, GRC might seem overwhelming. You probably have a lot of security practices that you're doing, but now you need to start documenting them because you'll have auditors coming in. It's kind of like taking a math class in school. You know that you have the answer right, but the teacher wants you to show your work.

The first step is finding a cybersecurity framework that works best for your business. Most frameworks include similar controls. On the other hand, some take a maturity model approach while others focus on risk-awareness.

Choosing a framework isn't always easy. However, if you're just getting started with cybersecurity compliance, you can consider the following:

- **Center for Internet Security (CIS) Controls:**
  Maturity-model approach with 18 categories of controls and layered safeguards
- **International Organization for Standardization (ISO):**
  Principles and practices for establishing repeatable cybersecurity processes
- **National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF):**
  Risk-based approach with five core functions that help define, iterate, and mature security

The good news here is also the bad news. Since every organization is different, no right choice exists. However, you should also consider where in the regulatory world each standard fits.

Regulations may or may not reference a standard, so you should review regulations before choosing a framework. The CIS Controls, ISO standard, and NIST CSF map to different regulations, but all three can be helpful if you need to comply with:

- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- Sarbanes-Oxley Act (SOX)

NIST SP 800-171 is a NIST Special Publication that provides recommended requirements for protecting the confidentiality of controlled unclassified information (CUI). Defense contractors must implement the recommended requirements contained in NIST SP 800-171 to demonstrate their provision of adequate security to protect the covered defense information included in their defense contracts, as required by DFARS clause 252.204-7012. If a manufacturer is part of a DoD, General Services Administration (GSA), NASA or other federal or state agencies' supply chain, the implementation of the security requirements included in NIST SP 800-171 is a must.

End of License

Reevaluating vendor relationships usually happens when your license is about to expire. You've been happy with your cybersecurity vendor, mostly. At least, you're pretty sure that you've been happy with them because you were on a multi-year contract. As the license is about to end, you're trying to figure out whether it's a relationship you want to continue.

Breakups are hard.

Like other companies, you're probably wondering how you want to approach this review. Some of the main questions companies usually ask at this point include:

- Is there a way to reduce costs with new technology?
- Is there something out there that's easier for my team to use?
- Can I find something that gives me a greater breadth of integrations?
- Are there other solutions that work better with my current technology stack?
- Is my current solution able to scale along with my cybersecurity needs?

At the same time, you're also trying to figure out if moving away from your current solution is worth the hassle. After all, implementing security technologies can take time and effort. Moving away from them feels like abandoning that investment. On the other hand, it might be time for you to say, "it's not you; it's me."

New to the Organization

Most organizations have at least some turnover. Whether you're a new CISO or security team staff member, you're looking to do the best job possible in this new role. You want to uplevel your current security posture, but you're not quite sure how.

CISO

You've been in your new role as CISO for a few months. Depending on the type of CISO you are, your responsibilities shift. You've done your gap assessment. You prioritized the controls that needed to
be updated sooner rather than later. You're still working on maturing the company's cybersecurity capabilities by growing out repeatable processes.

Now that you've put out any initial burning fires, you're ready to figure out what your role really is within the organization. According to **one global CISO survey**, you may either be:

- **Everything CISO:** Managing responsibilities across all three areas of security, risk, and trust
- **Specialist Role:** Managing responsibilities across only one or two of those areas

Maybe, your new company has a tool that you've had a bad experience with in the past. It might be that you experienced poor customer support. It might be that you have long-term plans that a current solution fails to help.

In either case, you know that you need *something* that gets you visibility into security while still being cost effective. With so many security technologies on the market, you're having a hard time figuring out the best way to optimize your spending.

Security Team Staff

It's nothing new that being one of the first security hires is challenging. Your new company is a great opportunity to grow, but they need to mature their security posture.

You've been in the field a while, but you also know that you have a lot more to learn about security. Many of the solutions on the market require a lot of time to implement. They also require a lot of specialized skills.

You're not alone. Security analysts are stressed out. According to **2023 Gartner research**:

- **25%** of Cybersecurity leaders will pursue different roles entirely due to workplace stress by 2025. Gartner predicts that by 2025, lack of talent or human failure will be responsible for over half of significant cyber incidents

Further, another 2022 study from **Tines** noted that:

- **27%** say their mental health has gotten worse over the past year
- A Gartner survey conducted in May and June 2022 among 1,310 employees revealed that **69% of employees** have bypassed their organization's cybersecurity guidance in the past 12 months.
- In the survey, **74% of employees** said they would be willing to bypass cybersecurity guidance if it helped them or their team achieve a business objective.

If you're someone who lives by the phrase "misery loves company," then there's a good chance you're in good company. If you want to reduce stress, then you need to find something that helps eliminate some — or all — of these issues with automation, AI and a platform for security or services that streamline security operations.

Budget Cycle

The annual budget cycle. It's that time of year again, and you need to review your current spending. At this point, you're looking at how you want to spread out your budget this year and over the next few years.

As you make your purchase decisions, you might be thinking about how to classify your expenditures.

- **Capital Expenditures (CapEx):** high upfront cost with depreciation over time
- **Operating Expenses (OpEx):** lower annual costs spread out over multiple years

Many companies are adopting cloud because it allows them to shift their spending models. With an on-premises solution, you put all your money on the table right at the beginning. You're going to be deducting the costs over several years because it's seen as continuously providing value. On the other hand, the value of the asset changes as it ages. This is great if you have the money and want to maintain the technology yourself.

Most companies are moving to cloud because it allows them to categorize the technology as an operating expense. You're paying an annual subscription fee, similar to paying your rent on an office space. Since you're not purchasing the asset, the subscription becomes a current expense. This changes how your company reports the expense on its taxes.

Choosing the Right Graylog for Your Budget Cycle and Needs

Graylog offers both an on-premises deployment and cloud-based option. If your procurement strategy focuses on CapEx for technologies, Graylog Enterprise gives you the on-premises deployment you need.

If you're reaching the end of your budget cycle but still want to uplevel your security, Graylog Cloud
is our cloud-based, subscription pricing option that provides all the features of the Enterprise option while offering the ability to reduce infrastructure costs.

Mergers and Acquisitions (M&A)

As your company looks to grow, you might be trying to incorporate new environments into your security program.

Mergers and acquisitions are hard. You've done the due diligence. You've reviewed the security posture. The problem is that you can't know everything until you're the owner. Whether you're merging with another company or acquiring one, the data they provided you only accounts for what they know.

Bringing together two different organizations means getting visibility into different IT environments. Maybe your current security technology doesn't play nicely with the deployments across the new organization. Perhaps, you just need to get the new organization onboarded quickly so that you have visibility as rapidly as possible.

You want to onboard all their systems, networks, security tools, devices, and users so that you can create a complete security program, aligned with your risk tolerance.

Using Graylog to Complete the Security Picture for M&A

Graylog is a vendor-agnostic solution that ingests all security event logs from all technologies. Our platform **supports many input types out of the box**, including:

- **Syslog:** TCP, UDP, AMQP, Kafka
- **Graylog Extended Log Format (GELF):** TCP, UDP, AMQP, Kafka, HTTP
- **AWS:** AWS Logs, FlowLogs, CloudTrail
- **Beats/Logstash**
- **CEF:** TCP, UDP, AMQP, Kafka
- **JSON Path from HTTP API**
- **Netflow:** UDP
- **Plain/Raw Text:** TCP, UDP, AMQP, Kafka

For any other add-ons, content packs, and GELF libraries, our **Graylog Marketplace** offers additional content packs that help you connect technologies and start analyzing security posture.

Strategic Initiatives

Strategic initiatives might mean one of two things:

- Your senior leadership and Board of Directors are building out their strategic initiatives and need you to manage the security aspects.
- You've put out all the initial fires and are now ready to build out a cybersecurity strategy.

Aligning with the Business-Level Strategic Initiatives

When businesses don't create strategies, they stagnate and stall. As your leadership builds out these future plans, they need you to determine how to align their business needs with protecting sensitive data.

Once you understand their goals, you need to find a way to align your cybersecurity strategies with theirs. Usually these include priorities like:

- Compliance
- Data security
- Reputation
- Availability and performance
- Cost effectiveness

Since the primary goal of business initiatives is to increase revenue, your alignment also includes proving that cybersecurity can be a **revenue enabler**.

Building a Cybersecurity Strategy

A strategic cybersecurity program often goes hand-in-hand with building out business initiatives. If you're being strategic with your security strategy, you're helping meet business goals like compliance, reputation, and data security with:

- Proactive risk management
- Situational awareness
- Crisis and incident response
- Supply chain management

Graylog: The Security Solution that Really Solves Your Problems

Graylog's platform gives you the robust capabilities you need to help you solve the biggest security problems you're facing. Whether it's trying to overcome the cybersecurity skills gap, looking to comply with mandates, seeking to reduce costs, or struggling to gain visibility, Graylog answers the call.

Reach out so that we can discuss your organization's security challenges how to proactively tackle them with the right SIEM platform and Threat Detection and Incident Response (TDIR) capabilities.

ABOUT GRAYLOG

Graylog is a leader in log management and Security Information Event Management (SIEM), making the world and its data more efficient and secure. Built by practitioners with the practitioner in mind, Graylog unlocks answers from data for thousands of IT and security professionals who solve security, compliance, operational, and DevOps issues every day. Deployed in more than 50,000 installations worldwide, Graylog is an award-winning platform built for speed and scale in capturing, storing, and enabling real-time analysis of terabytes of machine data. Graylog eliminates the noise and delivers an exceptional user experience by making data analysis, threat hunting, detection, and incident investigation fast and efficient using a more cost-effective and flexible architecture.

www.graylog.org
info@graylog.com | 1301 Fannin Street, Suite 2000, Houston, TX 77002

graylog

www.graylog.org
info@graylog.com
1301 Fannin Street, Suite 2000
Houston, TX 77002

graylog