BEHIND THE WHEEL

GETTING BEHIND THE WHEEL

Business Drivers for Security Purchasing

graylog

TABLE OF CONTENTS

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 eliminating 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. 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. Have you suffered a data security incident or breach?
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?

DATA SECURITY INCIDENT OR BREACH

The idea that a proactive security program is a robust program doesn't mean anything if you've experienced an incident or breach. Companies and IT teams know this already. In most cases, knowledge is power. However, sometimes it's just rubbing salt into a wound.

Why?

You're too busy implementing your **incident response plan** to think about the next steps in the immediate aftermath of a breach. You're still investigating your systems, trying to eradicate the threat actor and recover to a pre-attack state. Only when the digital dust settles that you have time to engage in your lessons learned analysis. At the same time, you have to find a way to prevent the same event from happening despite having just spent a solid chunk of change on responding to the data breach.

According to the **Verizon Cost of a Data Breach 2021 Report**, the average breach costs by category were:

AVERAGE COST OF A DATA BREACH

$1.24M	$27K	$1.14M
		
For detection and escalation	For notification	For post-breach response

Using the lessons learned analysis to determine how you can uplevel your security program and mitigate future risks, you need to consider some of the following questions:

- Did my team have the training needed to detect, respond, investigate, and contain the attack?
- Could the team have been better supported to detect suspicious activity?
- Do we have the reporting needed to identify threats, including monitoring and alerting?

When you look back at the incident, it's important to consider how you can better enable your team. Blaming the team doesn't do anyone any good. It's easy to blame human error when things go wrong. However, sometimes your technologies aren't giving your people what they need.

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)

Additionally, ISO and NIST CSF also map to the General Data Protection Regulation (GDPR). Meanwhile, suppose you're a Defense Industrial Base (DIB) member with the Cybersecurity Maturity Model Certification requirements hanging over your head. In that case, you will be focusing on NIST because NIST Special Publication 800-171 is now the official compliance mandate.

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 **research**:

- **70%** of security operations managers feel emotionally affected by their work
- **72%** of security operation center (SOC) teams

Further, security operations teams noted that:

- **40%** ignored alerts completely and world on something else
- **43%** walked away from their computers feeling overwhelmed
- **43%** turned of alerts
- **49%** assumed an alert was a false positive
- **50%** hoped another team member would step in to help

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 your stress, then you need to find something that helps eliminate some — or all — of these issues.

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.

MANAGED SERVICE PROVIDER VALUE

If you're an organization that chose to outsource your security monitoring to a managed security services provider (MSSP), it's possible that you're questioning all your life choices up until now. Outsourcing seemed like a great idea at the time, but you realize now that you have to manage the managed services.

If you have a smaller or less experienced security team, the MSSP was a great choice. You were able to use their technologies without worrying whether your team had the specialized skills that most security tools require.

Over time, you might have noticed that your MSSP:

- Has an interface you find difficult to use
- Sends too many alerts without offering context
- Lack the ability to provide a unified view across all your IT assets
- Inability to verify threat hunting capabilities
- Fail to provide response and remediation support

Frankly, you're at the point where you're starting to wonder whether you can bring your security operations back in-house. At the same time, you still have a limited staff who may not be able to do all the work on their own.

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.

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 2140
Houston, TX 77002