What Every Business Owner Needs to Know About Security in Their Organization

Sales and operations are top priorities for an owner working to build a business that runs efficiently — but now more than ever, the security of the company requires equal attention and care.

DOYLE®
Security for your life.™

Introduction

Business Owners are juggling so many business functions, they don't always have time to worry about the nuts and bolts of every department. But the rise of new kinds of security breaches, like phishing scams and ransomware, make security a pressing concern for executive leadership. And whether the risk is cyber or operational, every company — no matter how large or small — must take a holistic approach to mitigating security.

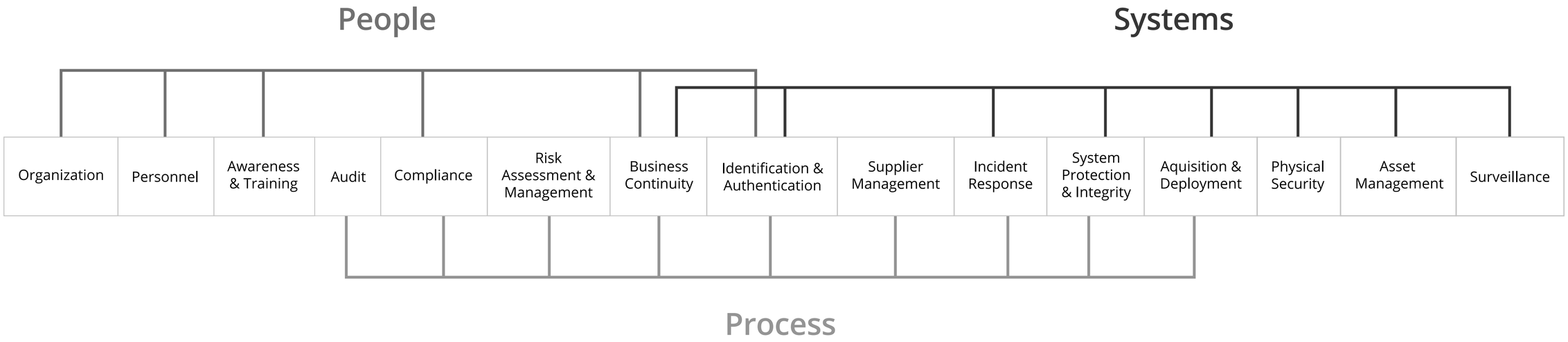
Owners who want to keep their company running without being breached must understand its security program. In this guide, we will identify the kinds of questions an owner should be asking themselves and their security and operations teams; and outline steps for planning a business security layout.

DOYLE®
Security for your life.™

Understanding the Security Framework

When outlining a new security framework, or simply trying to understand a company's existing one, it may be easiest to organize information using the common business approach of people, process, and systems.

A visual dashboard and ongoing reporting can keep a business owner informed of what security infrastructure is in place and what is missing. Owners should ask their security and/or operations teams to explain how the company's existing security program fits into the security framework below. It's important to note that this chart highlights the main areas relating to security and is a useful starting point, but a company's actual security framework may vary in sophistication based on its specific needs.



DOYLE®
Security for your life.™

Questions to Guide Security Discussions

A business owner can't know in detail everything that goes on in their organization, but they need to be able to ensure the right management staff is assigned to protect company data and assets.

Asking the right questions frames the entire conversation as an inquiry in which stakeholders are coming together to uncover the best solutions. Here is a list of questions to help owners guide security discussions, based on some of the top security challenges organizations face today.

Risk Assessment

Performing a risk assessment helps to identify, assess, and prioritize risks to the company in a relatively easy-to-understand format that empowers executive leadership. Questions to ask:

- Have you assessed your security risks?
- What security risks are most important to your company?
- Does your approach to security follow the priorities established in the risk assessment? If not, why?

People

All the technical security controls money can buy won't protect a company from operator errors. Often, the weak link in security is human, not technical. Questions to ask:

- How have you organized security in your company?
- Do you have a Chief Security Officer (CSO) or Chief Information Security Officer (CISO)? If so, who do they report to?
- Is there a risk that the CSO or CISO roles will be compromised because of where they report in the organization?
- How do you onboard new staff?
- Do new employees have appropriate levels of clearance commensurate for the work they will be performing?
- Do you require employees to comply with your security policies and procedures? If so, how?
- How do you provide security training?
- Is the training provided one time or on an ongoing basis?
- Are employees regularly made aware of new security risks and threats?

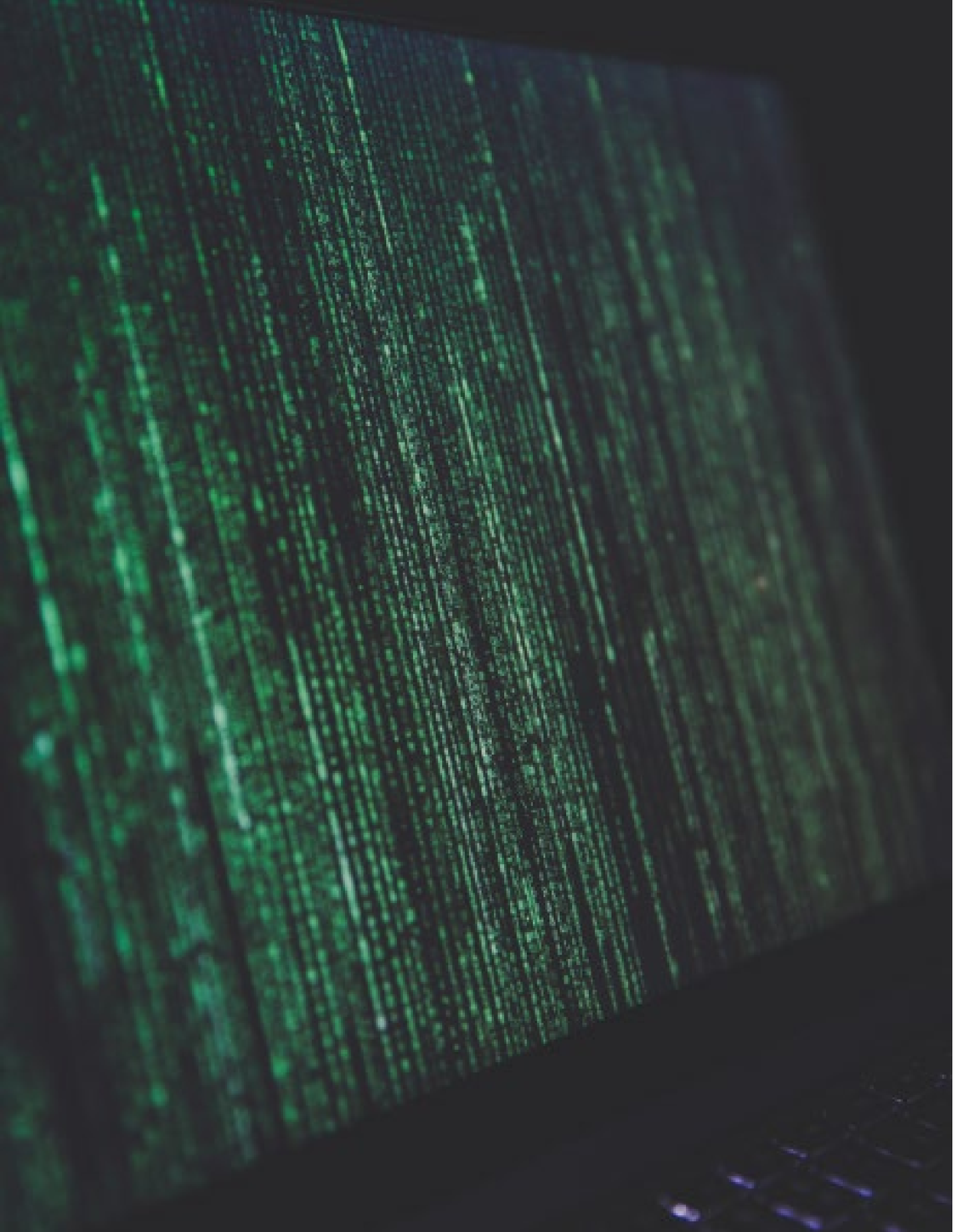
DOYLE®
Security for your life.™

Processes

Working to improve security processes is more successful when the work is done in close collaboration with the people who execute the tasks because they have the detailed information. This kind of information can be invisible to management, but is essential to implementing improvements. Questions to ask:

- Do you have written security policies and procedures, and do you follow them?
- Are the policies and procedures outdated, or are they used and updated frequently?
- How do you communicate security policies and procedures to the business?
- Do you audit security?
- Do you have processes to manage the application of your security policies and procedures with third parties?
- Is security incorporated into your business continuity planning?
- When you acquire products and services, do you formally consider the security ramifications?
- What process is followed when a security incident occurs?

DOYLE®
Security for your life.™



Systems

Systems are used to execute the process. The loss of any part of a supporting system can degrade or, in the worst case, eliminate the performance or capabilities of the whole security plan. Questions to ask:

- How have you addressed critical security and cyber security controls?
- Have you received a description of security tools being employed in terms that you can understand?
- Do your systems provide required access, no more than necessary, for authorized individuals? How is that done, in layman's terms?
- Are there risks with the way you grant access to your systems?
- Who is in charge of physical security? If not the CSO or CISO, how are physical security matters coordinated with the CSO/CISO?
- How do you do surveillance?

These are just some of the questions every business owner should clarify with their security team. Regularly engaging with those responsible for the company's security, and getting educated on basic security principles will help an owner to better balance risk and reward.

DOYLE®
Security for your life.™

Planning a Business Security Layout

Businesses are subject to various kinds of threats — from fraud, theft, and hacker activity, to even acts of terrorism. It behooves the owner or security management team to invest in adequate security systems to safeguard personnel, inventory, financial instruments, and records.

Creating a business security layout will help a company identify and assess those potential threats. And the best process for planning one involves developing a security master plan to outline security risks, goals, strategies, programs, and procedures.

Each company's security needs will differ, however, and its security layout will reflect the type of business it operates. For example, an online business will focus primarily on protecting digital data, while a brick-and-mortar business may be most concerned with physical security.

Developing a security layout takes careful planning, efficient processes, consistent implementation and ongoing maintenance. And most often, the effort is managed by either an outsourced security consultant, or in-house director of security, or both — but every owner should have a high-level understanding of what is involved.

Here is a simple breakdown of the steps for planning a business security layout.

DOYLE®
Security for your life.™

Understanding Key Business Goals

Security planning involves developing a company's security policies and applying controls to protect against potential threats. But the security planning process must be aligned with the company's strategic business plans so that it links with key business goals to add value and contribute to success. In other words: learn as much as possible about where the company wants to go, and create the security strategic objectives based on that.

For example, if building customer trust is a key business goal, security planning must include protecting customer relationships by safeguarding private customer information online and in hard copy documents. In this case the security layout must also include a secured area for customer records.

But reading the company's business strategy isn't enough. The security director or security consultant must involve other company stakeholders in the planning process to ensure that security is headed in the right direction and supported across the business.

DOYLE®
Security for your life.™

Evaluating Existing Security and Assessing Risks

Once the business priorities are identified, the next step is to conduct a risk assessment to figure out which security risks might keep the company from meeting its goals. The risk assessment is key to planning a business security layout, and should not be skipped.

The risk assessment is performed by the security director or security consultant and involves evaluating existing security policies, processes, and risks through information gathering. Owners, CEOs, CFOs, human resources directors, and facilities managers are interviewed to understand any history or potential of legislative requirements, hazardous materials, workplace violence, fraud and corruption, theft, extortion, acts of nature, or terrorism. Additionally, site and systems evaluations are conducted with key managers.

The risk assessment determines the cost of the impact of each identified risk and includes consideration of the physical safety of people on the premises, the company reputation, and delivery and production schedules.

Developing a Security Master Plan

A security master plan is a comprehensive strategy document that defines the company's long-term security goals, programs, and processes. It is used to guide the development and direction of security, consistent with the company's overall business plan. It also provides a detailed outline of the known risks and mitigation tactics over time.

The security master plan acts as a "playbook" of sorts, containing everything relating to security — including (but not limited to) information on security budgets expenditures, intellectual property protection, security guard staffing and assignments, locations of surveillance equipment, and/or areas secured with protective glass or temperature-controlled environments.

DOYLE®
Security for your life.™

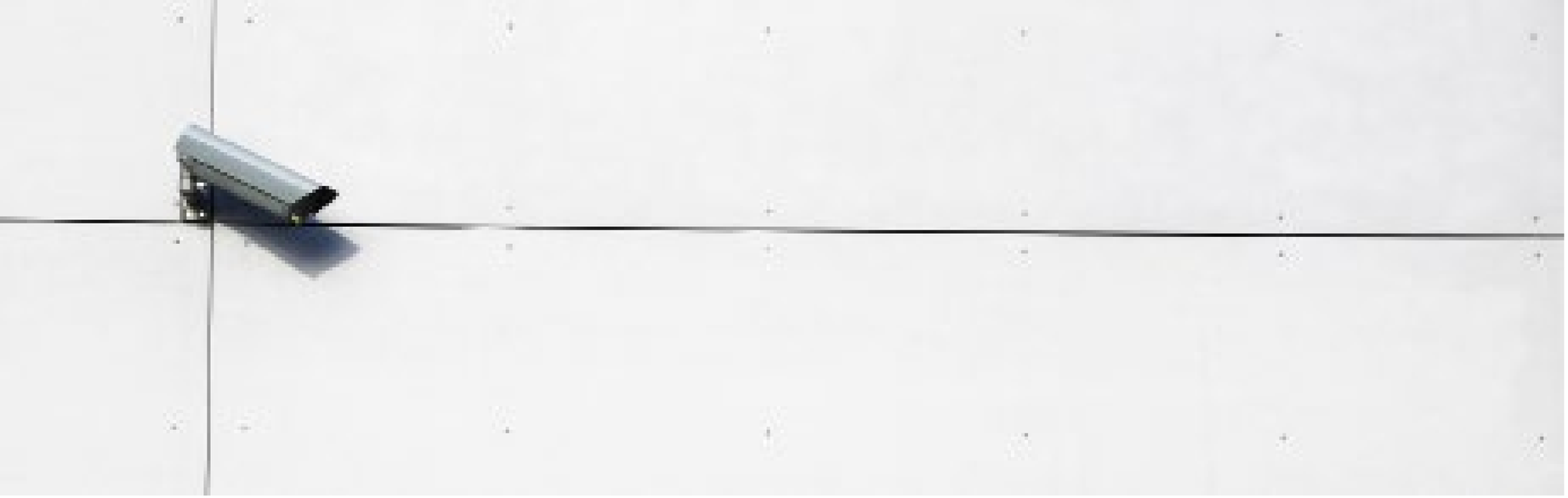
Testing and Maintenance

After the security master plan is developed, it will undergo a rigorous testing phase to surface any gaps or defects before it is approved for final implementation.

During testing, the security director and/or security consultant will walk through each section of the security plan with any security staff and document the testing process and results. In some cases, non-security employees will also walk through specific parts of the plan, to deliver a more robust testing result.

Once testing is complete, any problems found will be corrected and the master security plan will be updated to reflect the changes. And ongoing security maintenance will be scheduled and assigned to appropriate staff.

Product offerings evolve. Companies grow. Employees come and go. It makes sense to review and update the security master plan every quarter, to keep up with the pace of change. But it should absolutely be reviewed once a year at minimum. Just as threats and risk will shift over time, so too must a company's security master plan.



Conclusion

It is becoming critical for business owners to familiarize themselves with their organization's security policies and procedures, as they become increasingly accountable for any failures.

Being accountable doesn't necessarily require developing deep technical knowledge — it's about asking the right questions and understanding how the company's security approach relates to organizational and strategic priorities.

While owners can't know the inner workings of everything going on inside their business, they must protect their organization's data and property, preserve customers' trust, and manage costs and security resources wisely. The company's employees, reputation, and shareholders are counting on it.

DOYLE®
Security for your life.™

Want to Learn More About Business Security?

This e-book What Every Business Owner Needs to Know About Security in Their Organization is brought to you by Doyle Security.

Our company's focus is security and fire systems for Rochester, Buffalo, Syracuse Albany and Erie, PA businesses, but the information in this guide is meant to get you thinking about the kinds of security planning, processes, and technology needed to protect your business.

We hope it's helpful. In the meantime, we're here to answer any questions you have about security and fire systems going forward. Contact us at 1-866-GO-DOYLE or fill out a free consultation form on our website, www.GoDoyle.com

DOYLE®
Security for your life.™