WHITE PAPER

Do we need a SOC and if so, why?

Gradient CYBER

Gradient Cyber is a trusted cybersecurity partner operating primarily across the United States and specializing in small and mid-market enterprises concerned about cybersecurity but lacking the staff to give it the attention it deserves. For a fraction of the cost of hiring one cyber analyst our cybersecurity team is on the job 24/7 to improve your security, so you don't have to think about it anymore.

972-532-1878 • contact@gradientcyber.com • www.gradientcyber.com

TABLE OF CONTENTS

INTRODUCTION

Over the last several years, businesses have experienced dramatic increases in the number of cyberattacks impacting organizations of all types and sizes. The statistics reported in 2021 by the government, non-profits, and businesses involved in tracking cyber-crime are staggering. The FBI noted the highest number of complaints (847,376) and losses ($6.9B) due to cybercrime ever reported to them[i]. The Identity Theft Center noted the total number of reported data compromises is up 68% over 2020 and increased 23% over the all-time high[ii]. Changes in the way companies support employees, due to the pandemic, created new cyberattack opportunities and the criminal community has dramatically improved their ability to exploit the situation for financial gain.

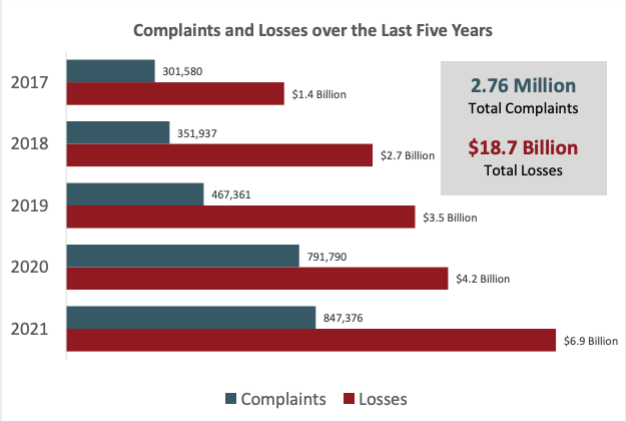

Figure 1 - FBI Internet Crime Report 2021

Small and midsize companies still think they are immune to cyberattacks, because they are not as attractive financially as their larger peers. The unfortunate truth is – the majority of cyberattacks happen to small and midsize businesses[iii].

Eva C. Velasquez

(President & CEO, ITRC)

January 2022

In 2021, there were **more data compromises reported** in the United States of America **than in any year** since the first state data breach notice law became effective in 2003.

Identity Theft Center 2021 Annual Data Breach Report

Cyberattackers have realized that attacks on smaller organizations can yield big financial gains and they encounter less resistance compared to larger organizations. The 2021 Verizon Data Breach Report showed that 56% of reported incidents impacted small business (less than 1000 employees)[iv]. Further research has shown that attackers use small and midsize companies as a cyberattack proving ground before moving on to their more difficult larger company targets, and/or a jumping off point to access networks of larger enterprises[v]. If your business is accessible through the internet in any way, then you are not immune to cyberattacks.

With the growing impact of cybersecurity attacks, it is critical that you are prepared to protect your organization, regardless of your business's size or industry.

While companies readily acknowledge that they must invest in fundamental organizational needs, such as accounting, facilities, and technology, they often do not consider cybersecurity to be mission critical to the business. Given the risk involved to the life of your business, it is important that cybersecurity concerns are properly addressed, by expert practitioners, just like every other core business function.

It is important to recognize the need to hire or outsource cybersecurity expertise, not just in the IT organization, but by management and the board of directors. In cybersecurity terms, this means your organization requires a Security Program and a Security Operations (SecOps) function or Security Operations Center (SOC).

> "The unfortunate truth is - the majority of cyberattacks happen to small and midsize businesses."
>
> Vistage Worldwide, Cisco, and
> The National Center for the Middle Market

THE CASE FOR A SECURITY PROGRAM

In addition to the obvious thwarting of observed threats to your business today, the implementation of a Security Program and Security Operations Center (SOC), can deliver other technical and business benefits to encourage your investment.

Preparing for and Meeting Compliance Mandates

Most businesses today fall under compliance mandates or exist in an industry that is creating new compliance structures.

For example, if your organization is in the financial services industry, you are impacted by FFIEC[vi] standards. In the healthcare industry, HIPAA[vii] standards apply. In the Defense industry, NIST 800-171[viii] or CMMC[ix] standards apply. If you process credit payments, then the industry-wide PCI[x] standards apply. Companies that do business with citizens of the European Union must accommodate GDPR[xi] standards. If you handle customer confidential data, many customers now require SOC-2[xii] certification. If you do business in or from the United States, you are very likely impacted by compliance standards that your organization should be addressing that has cybersecurity impacts.

After many decades of following large enterprises in the implementation of Security Programs, the US federal government has dramatically increased their focus and investment in implementation of security requirements. With the introduction of recent Executive Orders and Office of Management & Budget memos from both the Trump and Biden administrations, requiring the implementation of very strong security principles (such as Zero Trust Architectures), we are seeing most agencies take security concerns very seriously. This increasing focus on cybersecurity is having a follow-on effect on state and local governments and who are now imposing similar constraints on the hundreds of thousands of companies these agencies do business with.

A properly formed Security Program, supported by a Security Operations Center, will ensure that your organization is prepared to meet current and future compliance mandates allowing everyone to focus on revenue generating opportunities.

Addressing Supply Chain Cyber Risks

When you think about security, you most often think of securing your networks, software, and digital assets against cyberattacks and data breaches. But the supply chain - whether a traditional manufacturer, software provider, or service provider - is also vulnerable to security vulnerabilities, as has been identified as the source in a series of major data breaches.

Almost every organization is part of the supply chain, and supply chains are evolving to be as much about the flow of information as they are about the flow of goods and services. Thus, it comes as no surprise that supply chain security is a highly complex, evolving function, and it's one that security professionals and business executives are giving more attention as the risks facing information throughout the supply chain become increasingly obvious.

Supply chain security is every company's responsibility. The supply chain as a whole is only truly secure when all organizations carry out effective, coordinated security measures to ensure the integrity of supply chain data, the safety of goods, and the security of the global economy.

As a result, both government and commercial organizations are implementing new supply chain cybersecurity requirements. Companies are defining reasonable levels of security and associated controls; requiring sub-contractors, vendors, and critical supply chain partners to meet or exceed those standards as terms and conditions of established business agreements.

A properly formed Security Program, supported by a Security Operations Center, will position your organization to meet current and future supply chain requirements and to quite possibly win new business as a result.

Increasing Value from Existing Security Tool Investments

Most businesses have purchased products that provide security features. For example, firewalls, cloud environments, anti-virus software, active directory, and email systems (like Microsoft 365 or Google Workspace) all contain important features that should be enabled to provide very important security controls. Unfortunately, many businesses do not understand which features are appropriate in their environment and do not have the right options configured.

It is common for these deployed products to flag security issues that require attention in order to properly contain threats. This is usual for multi-pronged cyberattacks that attempt to gain access to your organization. In these cases, a product may flag an issue that highlights a problem that needs to be addressed using additional controls. If your company is not monitoring these generated alerts and responding to them adequately with best practices, then your organization is failing to obtain the full value of these products. In this situation, you are at an increased level of risk, as the products are not being fully used to detect and respond to threats.

But a properly formed Security Program, supported by a Security Operations Center, allows your organization to get full value from, use, and monitor these existing security products 24/7.

Incident Response Expertise When You Need It

Given the dramatic increases in cyberattacks worldwide, companies are discovering the need for security expertise in moments when the need is urgent, as they discover they are directly under attack. This specific situation is the worst possible time to frantically search for the right cybersecurity partner. Organizations that have not invested in the creation of a Security Program or not engaged a SOC find they don’t know where to start when situations escalate.

For this reason, it is important to identify your decision criteria and either hire your team to develop your Security Program and/or select your external partner(s). As a part of your Security Program, you will establish the plan to execute, should a significant security event ever occur. Establishing this program in advance also helps you to take steps to avoid many of these situations to begin with.

A significant advantage of engaging security partners early, regardless of how big or small the program, is to form a relationship of trust before you really need it.

In times of crisis, it is critical to have your own internal trusted resources or to have already established a strong relationship with external security professionals. That pre-existing relationship allows your team to respond much more quickly and cut through initial objections and issues of team dynamics. In the middle of a crisis, such as a security incident, cutting issue response times can significantly limit the scope of damage the attacker can inflict.

THE IMPACT OF DELAYING OR DOING NOTHING

As in all important business decisions, some members of your organization may encourage the team to delay or defer investments in security or to frankly do nothing. While this may seem attractive from a cost standpoint, it is highly recommended that your organization start the process of building your security capabilities, both Security Program and Security Operations Center support as quickly as possible. Why?

Not Being Able to Identify Current Security Posture Weaknesses
Gradient Cyber conducts risk and threat assessments for small and midsize enterprise organizations every month. And while all organizations are different and their business models vary, common issues show up regularly that create major security posture weaknesses. Examples of common security posture weaknesses include:

- **Network Configuration Issues** – External attack surface configuration issues like unencrypted / unsecured services exposed on the Internet (e.g.; FTP, Telnet, RDP, SSH, POP3, SQL, MYSQL, etc.)

- **Unsecure Application Exposures** – Unsecured applications that are mistakenly exposed to the Internet (commonly this is applications designed for internal use being exposed outside the organization).

- **Unsecured Shadow IT** – Unsupported and unknown operating systems and applications in use that are not secured or patched.

- **Email Login Credentials Exposed** – Unknown corporate email data breaches where email addresses, passwords and accounts are available on the dark web to malicious actors.

- **Possible Data Leakage** – Private information is exposed like financial data, company intellectual property, and personally identifiable information.

- **User Enumeration** – Applications that, in response to a failed authentication attempt, return a response indicating that the username is correct, and that the authentication failed due to an incorrect password, making brute-force login attempts much easier.

If these unknown weaknesses are allowed to persist and go unaddressed, companies needlessly leave vulnerabilities exposed to attackers that could otherwise easily get fixed.

Not Having Continuous Security Monitoring to Detect Security Threats

In late 2021, a critical issue was discovered in a Java logging module, known as log4j. This issue was very easy for attackers to take advantage of and left hundreds of millions of devices[xiii] vulnerable for attackers to compromise. Organizations of all sizes experienced outages and breaches as they raced to resolve the log4j issues before they were compromised. Many believe that this issue will continue to be exploited by attackers for several years. Without continuous security monitoring, organizations remain exposed and vulnerable to all sorts of attacks like this example.

Not Being Prepared to Respond Quickly to Broad Scale Attacks

The year of 2021 saw some of the most dramatic broad-scale internet attacks that the industry has ever seen. Issues such as the Microsoft Exchange Server Vulnerability[xiv], initially known as Hafnium, exposed up to 60,000 organizations[xv] to very damaging cyberattacks against their email systems. Criminals from external locations were actively searching and compromising thousands of systems over the course of several months and all organizations that hosted their own Microsoft email services were scrambling to protect themselves.

Without a Security Program or Security Operations Center focused on threat response, organizations remain unnecessarily exposed to issues that require quick and disciplined response in order to minimize the likelihood of a breach, like this example.

Attacks like these continue to increase across all industry segments. The longer you defer investments in your Security Operations efforts, the more exposed your organization will be to new cyberattacks. And as is the case with all great endeavors, success must start with one small step. Thus, we recommend you start, however small, just start none the less.

THE COSTS OF GETTING STARTED

The cost of a full Security Program can be significant, unless they are carefully managed. When compared to the cost to the business or the life of the business should a major cybersecurity event occur, getting started with a Security Program and Security Operations Center can be quite small.

In fact, the recommendation is to start small whether internally, or with a security operations vendor, to learn as you go. Experiment and scale what works. Below are a few points of guidance to help get the most "bang for your buck."

- **Leverage Existing Security Tools** – Ensure your plans or your vendor's plans incorporate your existing toolsets and do not require unforeseen additional product purchases. This keeps initial costs to a minimum.

- **Focus on the Ability to Scale** – Does it make sense to bring on dedicated resources for the scale of your organization, or can you bring in a security operations vendor focused on serving your size of organization? Whichever route you go, ensure you can grow easily over time, both in scope and scale.

- **Focus on Fit for Purpose** – Find a Security Plan and Security Operations solution that meets your organization where you are – both in experience level and financial resources.

- **A Willingness to Continuously Improve** – Develop a culture that looks to continuously improve and a Security Plan and Security Operations solution that can walk with and teach your organization as you strive to improve overall cybersecurity and drive best practices.

NEXT STEPS

The nature of the ongoing threat landscape has escalated the issue of cybersecurity into the board room of organizations. It is no longer possible to ignore the risks or to assume that cyberattackers will not eventually impact your organization. Combined with the overall business value, each organization should decide that now is the time to take necessary steps to build a Security Program that includes a Security Operations Center (SOC). Once you decide to move forward, it is time to understand the options that are available to you and how they fit your business requirements.

See white paper #2 titled "What is a SOC and What Benefits Can We Expect?" in which we review the technical features and business benefits your business should look for when evaluating SOC alternatives.

---

i Federal Bureau of Investigation Internet Crime Report 2021

ii 2022 ITRC Annual Data Breach Report

iii Cyberthreats and solutions for small and midsize businesses, Vistage Worldwide, 2018

iv 2021 Verizon Data Breach Investigations Report

v 2019 Verizon Data Breach Investigations Report

vi Federal Financial Institution Examiners Council

vii Health Insurance Portability and Accountability Act of 1996

viii National Institute of Standards and Technology Special Publication 800-171: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

ix Cybersecurity Maturity Model Certification

x Payment Cards Industry (PCI) Security Standards Council

xi General Data Protection Regulation for the European Union

xii Service Organization Control 2, Association of International Certified Professional Accounts

xiii The Log4j Will Haunt the Internet for Years. Wall Street Journal.

xiv Microsoft Exchange Server Vulnerability CVE-2021-42321

xv Microsoft was warned months ago, The Verge