Flosum

The State of Cloud Security 2022

Cloud Security in 2022

Each year brings new hope and new challenges, and 2022 is no exception. While the world is still reeling from unprecedented times, companies are continuing to adjust to a diverse workforce that has settled into a routine of remote staff and essential field personnel. Zoom calls, instant messaging, shared files over cloud networks, and remote collaboration have become the norm.

Companies continue their struggle to protect information over networks with daily challenges. A one-size-fits-all approach to security is impossible. A company cannot purchase a package off the shelf and expect it to meet their needs instantly.

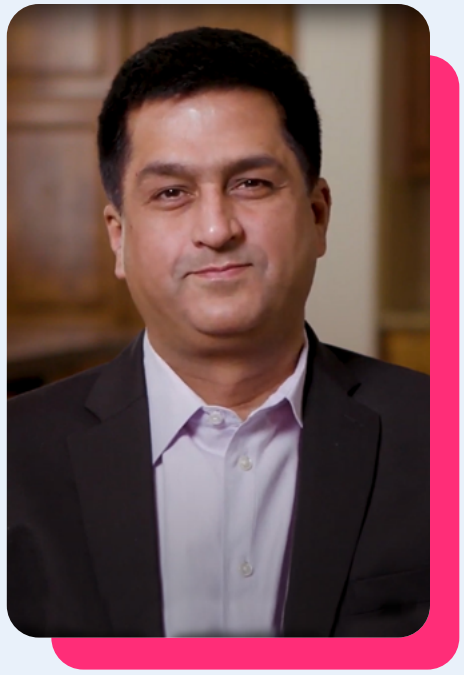
With the vast amount of information in the cloud and the increased level of global security threats, companies need to expand and protect in order to thrive. While some executives still have reservations about cloud security, Flosum is here to earn your trust and enable you to create trust within your organization.

We hear your concerns and have developed one of the most robust systems available to protect your networks. Flosum is doing everything it can to protect data and drive innovation, but we can't do it alone.

Security is complex. In-house security is just as important as cloud security, and having your data in the cloud does not eliminate the need for internal measures. Success in security is dependant on a shared sense of responsibility - one where the company, suppliers, employees, contractors, and customers all work together toward a common goal.

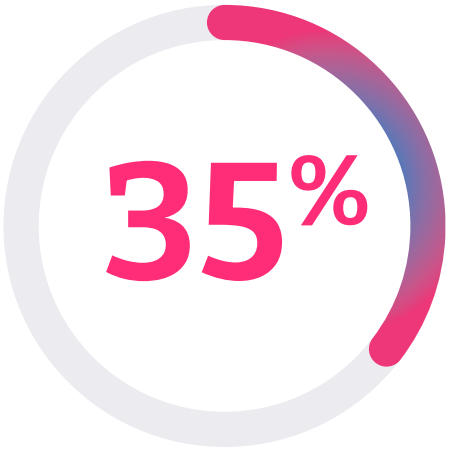
We have compiled and published this authoritative report on the State of Cloud Security: 2022 to enlighten and empower you and your team in this shifting digital world. Together, we can create an environment that addresses security threats and fosters innovation.

Thank you.



Girish Jashnani,
Flosum CEO

Cyberattacks on the Rise[1]

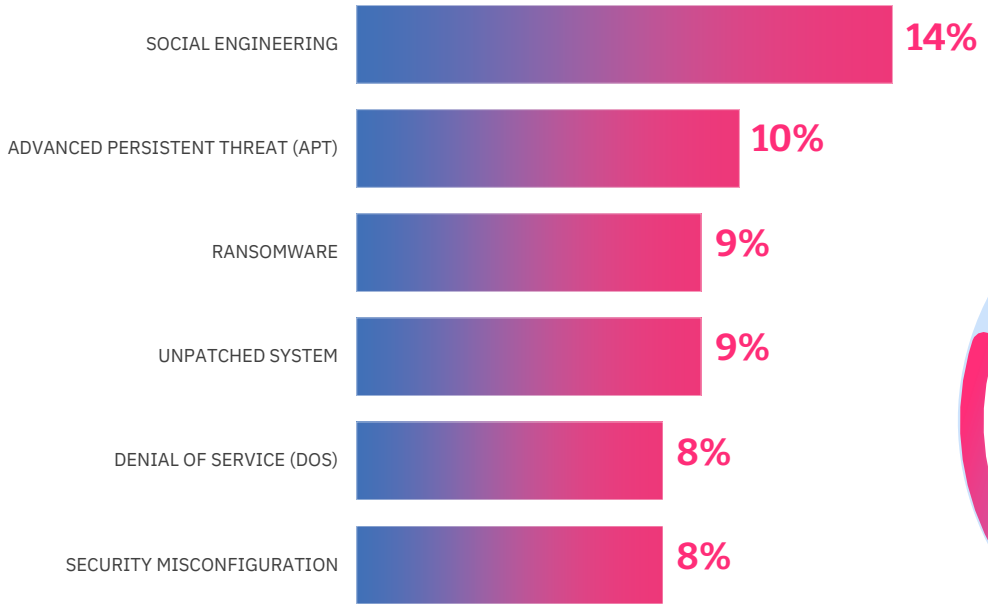


Enterprises reported a 35% increase in attacks this year.

Before delving into cloud security trends, the following security insights lay the groundwork for a broader approach as well as an understanding of organizational and individual concerns people may have when it comes to security in 2022. Leading research reveals many commonalities in security trends. One of these is the need for protection from cyberattacks. This threat is constant.

Top security challenges and events in 2021 included Solar Winds, Colonial Pipeline, Log4j, Kaseya, as well as many more. The next imminent threat has companies on edge. More than one-third of all enterprises noticed an increase in attacks and that number is expected to rise. Of particular concern are infrastructure and supply chains already weakened by pandemic concerns.

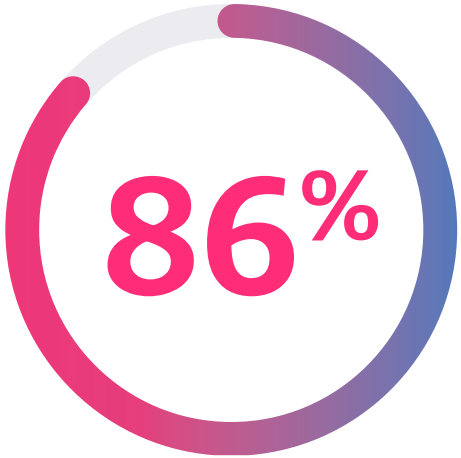
Most Frequent Types of Cyberattacks Experienced

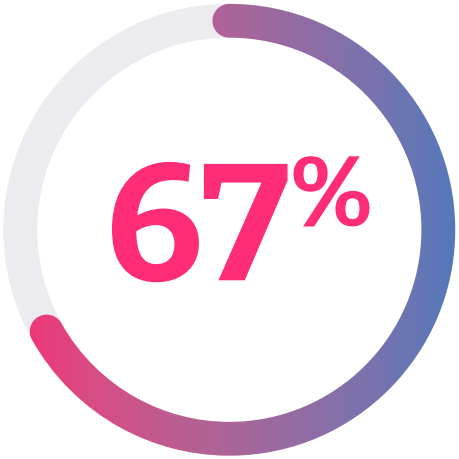


No One is Immune to Security Attacks

While there is much publicity surrounding the major attacks suffered by big tech companies, attacks are not limited by business size. 43% of attacks are aimed at small and medium-sized businesses, but only 14% have adequate tools in place to defend their networks.[2]

In 2021, at least one person clicked a phishing link in around 86% of organizations.[3]

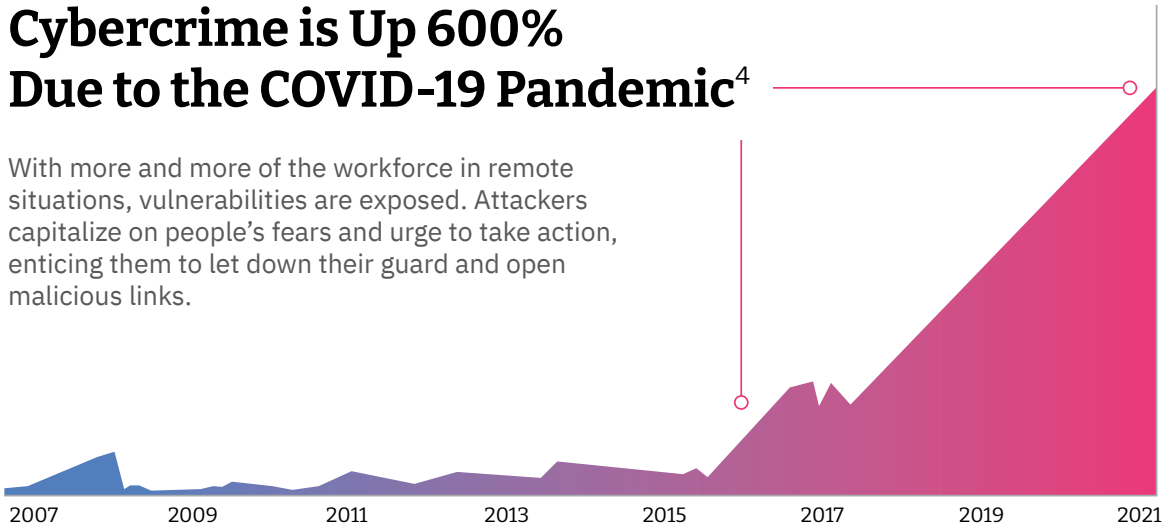




67% of leaders are wary of cybersecurity risks.[2] While this may translate into the frightening realization that many leaders are not at all prepared for attacks, it also indicates a willingness to take action to shore up networks and practices.

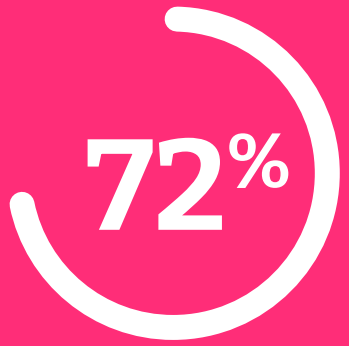
Cybercrime is Up 600% Due to the COVID-19 Pandemic[4]

With more and more of the workforce in remote situations, vulnerabilities are exposed. Attackers capitalize on people's fears and urge to take action, enticing them to let down their guard and open malicious links.

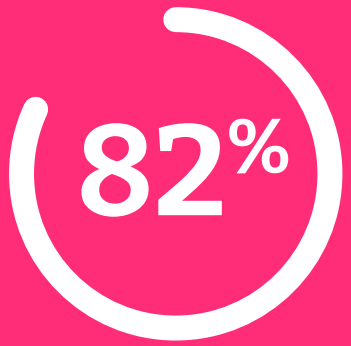


Leader Readiness On Security[1]

Less than 57% are ready to have board-level security conversations.



More than 72% feel that their security configuration has drifted from their gold standard.



More than 82% don't have adequate resources allocated to maintain security.

Are Your Security Levels Ready?

With the publicity of security breaches and the potential loss of revenue, it is surprising that so many companies have not made network security a higher priority. More than 82% of companies do not have adequate resources allocated to maintain security.

Understanding the benefits of security investment is crucial. Besides curbing revenue loss, security enhancements:

- Help companies gain a competitive edge by building trust
- Ensure compliance with government agencies
- Allow for a more proactive approach to threats and a quicker response
- Prevent insider threats

Board members must ask the tough questions:

- Are we 100% secure? Are we sure?
- How bad is it out there? What about what happened at X company? How are we doing compared to others?
- What is our weakest link?
- Do we know what our risks are? What keeps you up at night?
- Are we appropriately allocating resources? Are we spending enough? Why are we spending so much?

Cloud Security is a Global Priority

There is a need for more global collaboration to address cloud security. Following is a collection of insights from cloud security experts. [5]

"I think the first thing we need is more young people going into computer science, trained in something technical and exposed to computing. That period of time [after high school] should be a period of national service. A really scalable CyberCorps program, something meaningful."

Ed Amoroso, CEO and founder of TAG Cyber Security

"Detect and protect. We do need to simplify things. We're all connected to each other."

Taher Elgamal, CTO for security at Salesforce

"Builders don't think like breakers. They're not incentivized to do the same things. And that's just a fact."

Casey Ellis, founder and CTO at BugCrowd

"You don't get demoted by creating a product that has a security flaw; you get promoted by having the functionality that can sell. Minimum viable product is going to get you maximum security exposure."

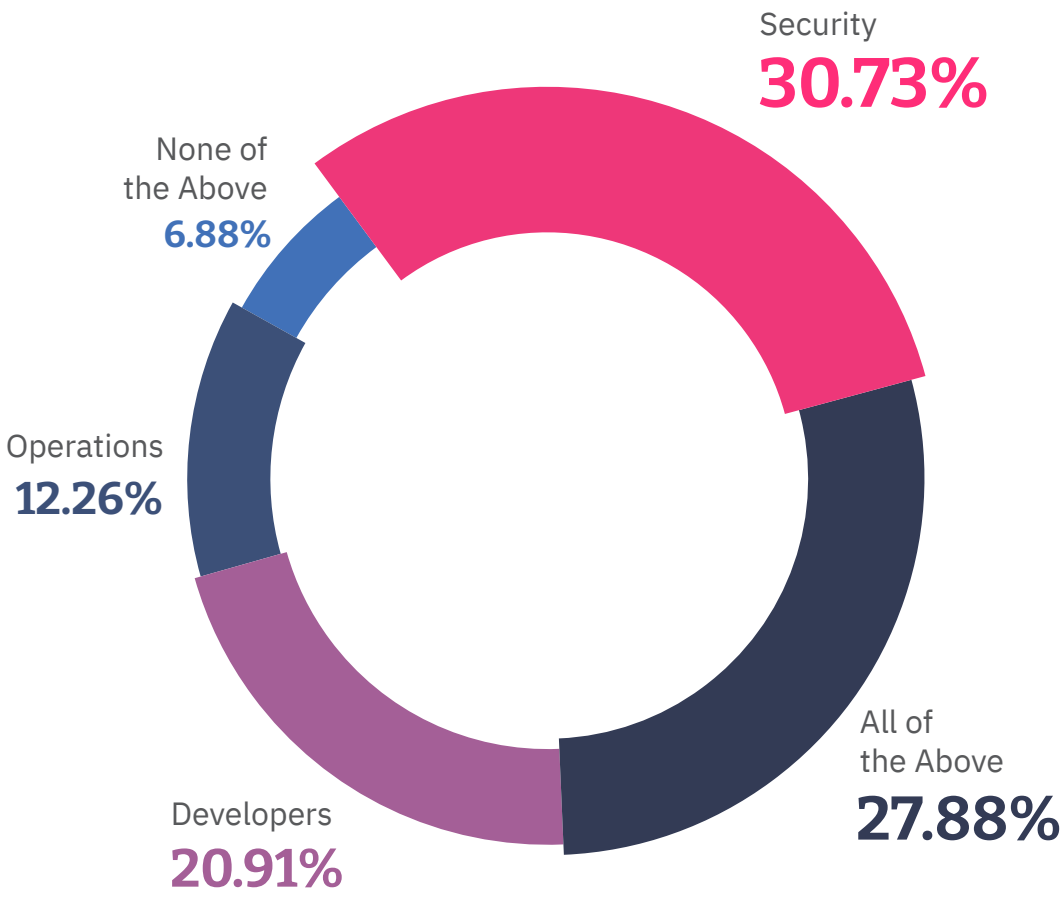
Malcolm Harkins, chief security and trust officer at Epiphany

Collaboration with Security Teams

Security teams pore over cracks in the system, reinforcing the firewall, and anticipating where the next threat will occur. These efforts are to be commended, but they can't do it alone. One employee can unwittingly cause a breach in the system or stop a threat in its tracks.

Companies that employ a uniform approach to security are the most successful. Everyone who touches a network has a vested interest in its success. The security team may be on the front line, but all members of an organization ensure its success.

In Your Organization, Which Group is Primarily Responsible for Security? [6]



Privacy Controls

Once trust in a company is breached, it is almost impossible to earn it back. 84% of consumers indicate that high-security controls are near the top of their list of reasons for choosing a company to do business with. Nearly half of consumers have switched loyalties to brands due to privacy concerns. How a company responds to a threat can make a difference in whether the customers bail or give it a second chance.

Flosum and its partners work together for the common good. When one faces a threat, there is a spirit of sharing and collaboration to ensure the threat is identified and eliminated across all platforms.

How Consumers Feel About Data Privacy

Just 10% of consumers feel they have total control over their personal information.[7]

10%

88%

88% of consumers say the extent of their willingness to share personal information is based on how much they trust a company. [7]

92% of consumers say companies must be proactive about data protection. [7]

92%

48%

48% of consumers have stopped buying from a company over privacy concerns. [8]

Zero Trust Compliance

One approach to preserving customer privacy is to implement a Zero Trust plan. Executive Order 14028 from the President of the United States is called "Improving the Nation's Cybersecurity" and requires agencies to submit an implementation plan for Zero Trust. This plan needs to be submitted to the Office of Management and Budget (OMB) and Cybersecurity and Infrastructure Security Agency (CISA) for review. Furthermore, by the fiscal end of 2024, agencies must be compliant with the Zero Trust Maturity Model.

Zero Trust requires that:

- All users in an organization, whether they are in or outside the network, must be continuously monitored and the user's access privileges validated.
- The impact of an internal or external breach must be minimized.
- For the most accurate response to a breach, companies must automate their context collection and response.

This approach is significantly different from traditional verification processes and provides better protection over the cloud. It recognizes that a breach can occur at any point in the process and a continuous verification at all access points alleviates these threats.

Zero Trust solutions can take on many forms depending on the complexity of your network, but it is essential for compliance and security.

Global Privacy Laws and Regulations

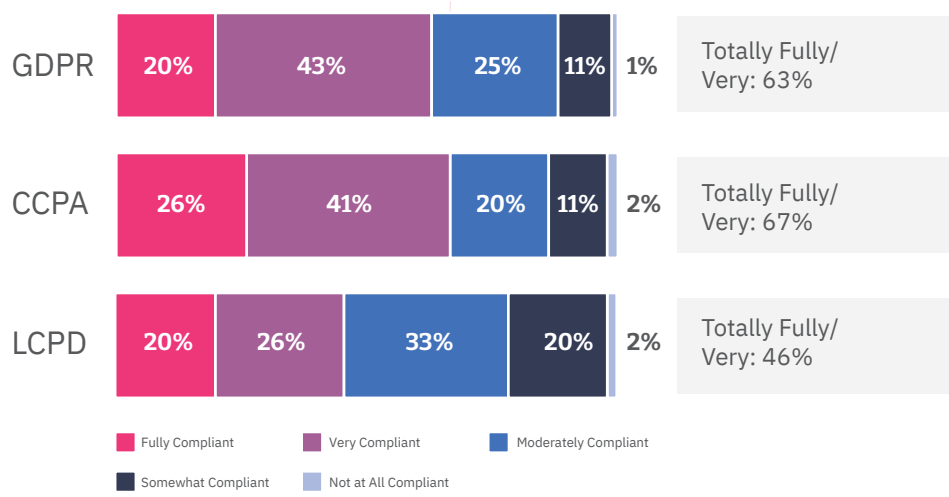
GDPR was put into place to protect information, including web data, basic identifying information about consumers, and more. Other regulations abound. Last year, California voters passed the California Privacy Rights Act (CPRA), on top of the existing California Consumer Privacy Act of 2018 (CCPA). And Brazil's General Data Protection Law (GDPL) marks the country's first law to provide a comprehensive framework regulating the use and processing of all personal data.

Whether your business touches European shores or not, you are affected. Non-compliance holds a hefty fine of up to 4% of a company's annual global revenues or 20 million euros ($22.8 million), whichever is higher. In the past year, these fines have equated to $1.2 billion in fines. While most of these fines are on big tech giants, anyone who has an international supply chain and data transfers must follow the regulations.

It is in a company's best interest to develop a plan, whether the compliance approach is a global strategy, handled according to local, applicable laws or simply a local strategy. In addition to being a prudent business practice in the way companies handle your data, compliance builds trust.

Compliance with GDPR, CCPA and LGPD[9]

(Base Law Applies)



Non-Compliance Can Result in Fines of Up to

$22.8 M

Questions to Ask Your Organization

01

What kinds of personal information does our organization process?

02

Where do we store this data?

03

Who can access this information?

04

Do we transfer personal information among different systems or stakeholders groups?

05

How is this data secured?

06

Do we obtain consent to store personal information, and if so, how and where is it documented?

07

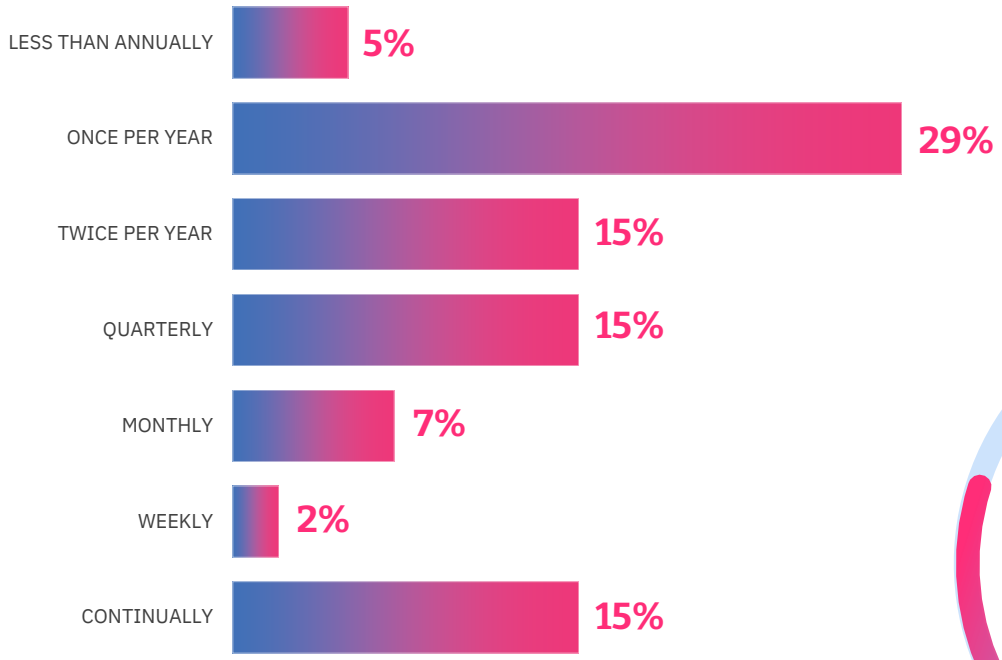
Do we have official processes or policies related to the collection or use of personal data?

Enhanced Security Training

In order to combat the constant threats that bombard your organization, security awareness needs to be a priority. Many companies require a boxed training session once a year that includes generic questions on phishing, malware, using passwords, etc. Others publish guidelines including requirements for employees to read.

This is a start but may leave gaps. Cyber criminals employ new tactics all the time, and everyone must be prepared. A comprehensive training plan might include periodic updates from the security team, short reminders on best practices, requiring more frequent password changes, or test phishing emails sent randomly to keep everyone on their toes. Make security awareness a top priority starting at the executive level.

Frequency of Employee Cyber Security Training[10]



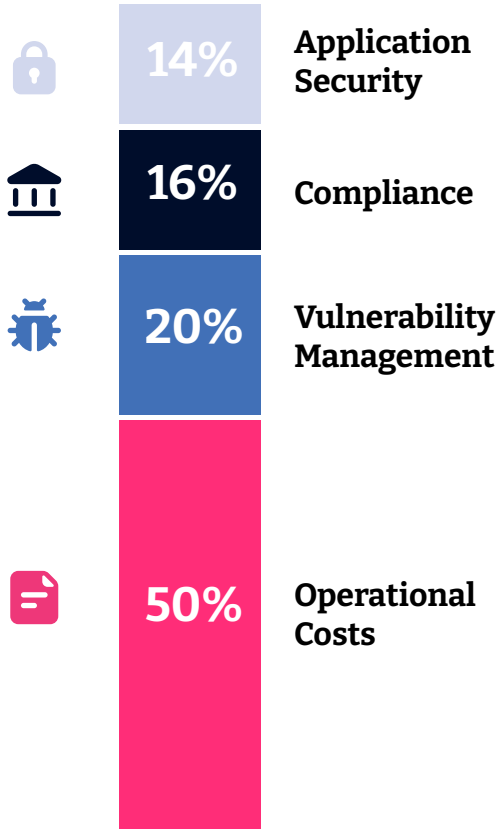
Prioritize Security in Your Budget

In order to set your organization up for success in the security arena, adequate resources must be allocated in your budget. Considerations must be given for physical security as well as cybersecurity. Physical security may include access controls to sensitive areas, insurance, and a dedicated security staff. Cybersecurity includes network controls, firewalls, access to data, and compliance requirements for government regulations.

Areas to focus on include providing for the protection of physical assets - buildings, inventory and data, implementing security software, setting aside growing room for enhancements, developing a business emergency plan, and employing proper training. Having a budget helps you prepare for the unknown and provides peace of mind; it helps set clear goals.

While there is no set formula for creating a security budget, a Gartner report[11] breaks down an average company's security budget into these categories:

Average Company's Breakdown of a Cyber Security Budget



Key Recommendations

Keeping up with cybersecurity is a daunting task, but there are tools and practices that increase your network protection immensely.

01 Automate Security Operations

Equip your security personnel with tools that will help them do their job. These tools monitor constantly, are able to detect threats and can execute mitigation actions behind the scenes, leaving humans to tackle the bigger tasks. Automation can also standardize security processes and create consistency in responses.

02 Improve Collaboration Between Enterprise Security & Cloud Teams

This involves both teams working together to pinpoint threats and close gaps. Chances are, you are not the lone enterprise experiencing a security threat or bottleneck. Working with Flosum enables solutions.

03 Adopt “Always On” Security & Zero Trust Maturity Model

We’ve mentioned Zero Trust in terms of compliance and importance. Those that intend to do harm do not rest and that means you can’t either. Continuously improve your practices and you’ve got a great chance of coming out on top. Use the model as a guideline.

Citations

[1] State of Cybersecurity 2021, Part 2: Threat Landscape, Security Operations and Cybersecurity Maturity, ISACA, 2021.

[2] Ninth Annual Cost of Cybercrime Study, Accenture, 2019.

[3] Cybersecurity Threat Trends, CISCO, 2021.

[4] U.N. disarmament chief Izumi Nakamitsu, UNSC Arria-formula meeting on “Cyber Stability, Conflict Prevention and Capacity Building”, 2020.

[5] Salesforce 360 Article “Cloud Security Is a Global Priority: How Can IT Leaders Protect Our Future?”

[6] A Maturing DevSecOps Landscape 2021 Global Survey, GitLab.

[7] PwC Cyber & Privacy Innovation Institute.

[8] Pew Research Center Survey, 2019.

[9] IAPP-EY Annual Privacy Governance Report 2021, iapp and EY, 2021.

[10] Employee Cyber Security Awareness Training Frequency in Organizations in the United States as of 2018, Statistica, 2022.

[11] IT Key Metrics Data 2019: Key IT Security Measures: by Industry, Gartner, 2018.

About Flosum

Flosum is a leading provider of end-to-end secure DevSecOps, data management, data protection and security automation platforms, built 100% natively to Salesforce.

Our mission is to enable IT leaders to manage the cloud with confidence and empower developers to innovate using Flosum's release management, Salesforce data backup and recovery and Salesforce security solutions. Enterprises around the world leverage Flosum to accelerate digital transformation by making the software release process fast and easy and increasing developer productivity while remaining secure and compliant.

More information can be found at:
www.flosum.com