RESOURCE CENTER

What are security controls?

Commonly overlooked areas when establishing security resilience at work and at home.

Get the full interactive view at
https://bitwarden.com/resources/what-are-security-controls/

bitwarden

What are security controls?

Security controls are the backbone of any robust security strategy, serving as the measures organizations implement to safeguard their assets — people, property, or data — from a myriad of security risks and threats. These controls are meticulously designed to prevent, detect, counteract, or minimize the impact of security incidents on physical property, information, computer systems, or other valuable assets. By understanding and implementing effective security controls, organizations can create a fortified environment that ensures the safety and integrity of their operations.

SaaS landscape and the state of BYOD

Bree Fowler, senior writer at CNET, led a panel discussion at the 2024 Bitwarden Open Source Security Summit between Schlomo Schapiro, principal engineer at Tektit Consulting, and Bjoern Sjut, managing director for productivity and IT at Front Row. The conversation explored the current trends and challenges of security resilience and employee adoption. It featured recommendations from both experts on how to improve overall security through strategic and thoughtful security controls.

Schapiro started the conversation by underscoring the threat posed by software-as-a-service (SaaS) technologies.

> **"Most companies completely ignore or underestimate the threat posed by their current SaaS landscape," said Schapiro. "They essentially put blind trust in their SaaS vendors and give up full ownership of their perimeter. It's one of the biggest mistakes companies make. They let their perimeter become a thin fence with lots of holes, which are ultimately holes that hackers can exploit. As an industry, we need to catch up with reality."**

Sjut also highlighted the importance of perimeters, noting the huge shift towards cloud applications has made perimeters more opaque. His main concern, however, lay in the fact that people are much more mobile. "If we don't want to arm everyone with dedicated, specific devices, we have to deal with the challenges posed by a bring your own device (BYOD) environment. In conjunction with these cloud tools, it means we have more attack vectors on the devices and through applications."

While BYOD devices can pose security risks, organizations can bolster their defenses with tools like password managers. Bitwarden offers cross-platform access for mobile, browser, and desktop applications, enabling an environment of unlimited passwords and devices.

https://player.vimeo.com/video/1015905668

Watch the session

Table of Contents

What are security controls?

SaaS landscape and the state of BYOD

Putting the pieces together to balance security measures and productivity

Security awareness training: Mitigating friction while accounting for human vulnerabilities

Mistakes companies make when establishing security resilience - and what they can do differently

What are the types of security controls?

Get started with Bitwarden

Putting the pieces together to balance security measures and productivity

Most organizations grapple with many moving parts to strengthen security. To prevent important things from falling through the cracks, Shapiro believes that “companies need to ensure that every application introduced into their stack uses federated authentication against

their primary identity provider. One of the worst-case scenarios is having accounts or applications that aren't well understood, which stay active after an employee has left the organization."

Sjut emphasizes that security should not be restricted to "an enterprise feature. As an industry, we should all advocate for built-in security so we don't end up in a position where we have to plug holes with many different measures."

Security professionals must put all the pieces together and figure out what works best for them. Controls are essential to mitigate business risks and ensure security effectively.

> "We want to find the right balance between security and productivity. I think a mistake many companies make is putting a security goal on the agenda that can lock people out of being productive. This makes them less secure in the long run because employees build up their own shadow IT that is completely outside the bounds of company security controls. In our view, it's about balance, coupled with a risk-based approach." ~ Bjoern Sjut

If organizations want their security departments to be effective, they must embrace and enable users to do their jobs efficiently.

> "It's always important to be approachable as an IT department. You want to create an environment where the path of least resistance from the user doesn't circumvent your security." ~ Schlomo Schapiro

Employees who cannot share relevant work files with clients or team members are more likely to circumvent security protocols. The only way to protect against that is to ensure "employees feel supported in their productivity. It really is about collaboration and finding the right balance between productivity and security (Sjut)."

Password managers can help users navigate the tightrope of security and productivity. They offer a fast and efficient avenue for creating, managing, and securing passwords. Reputable password managers such as Bitwarden also include MFA tools users can leverage for an extra layer of security, like the built-in Bitwarden Authenticator or the stand-alone Bitwarden Authenticator app.

Read more:
How to build the best cybersecurity tech stack for your business

Security awareness training: Mitigating friction while accounting for human vulnerabilities

People naturally tend to avoid friction, including friction caused by security policies. Fowler asked Schapiro and Sjut how they best incentivize employees to avoid circumventing security best practices.

> "My personal recommendation is to think of your users as citizen developers. It is important to enable your employees to make use of the systems you provide. It is important to be approachable, reach out with a helping hand, and put user enablement first."

> ~ Schlomo Schapiro

Sjut noted that in many companies, it can be challenging for users to figure out how they should get access to a tool they need. This is particularly prevalent in mid-size companies because the company may be large enough to lose sight of all the tools available but not large enough where there is corporate oversight.

> "In my opinion, a lot of companies manage their IT incorrectly. They don't manage it as a defender of the status quo. They manage it more as a facility management unit to keep the lights on. Very few IT organizations have the goal of making people more productive." ~ Bjoern Sjut

Mistakes companies make when establishing security resilience - and what they can do differently

Schapiro emphasized the importance of having control over SaaS perimeters and having a solid plan in place for retrieving backups – including routine test runs to make sure everyone understands their role. Organizations must focus on protecting and maintaining critical systems to prevent breaches and ensure they remain functional and secure against potential attacks.

Sjut said that in addition to backups, many companies don't really have a robust understanding of identity, including with people they collaborate with such as freelancers.

"The amount of personal Google accounts used to manage Google Analytics data is baffling to me," said Sjut. "Most companies need to deal with digital identities. My general sense is that there's rarely someone who feels responsible for digital identities within the organization. Businesses need to understand their core identity provider, how the identities work, and if they have them under control. The more people log into cloud applications on a personally owned device without the employer understanding that identity, the more difficult it is to mitigate damages."

What are the types of security controls?

Physical security controls

Security controls can be broadly categorized into three main types: physical, technical, and administrative controls. Each type plays a pivotal role in creating a comprehensive security framework. By integrating these three types of controls, organizations can create a multi-layered defense strategy that addresses various security aspects.

- Physical controls include measures like access control systems, surveillance cameras, and alarm systems.
- Technical controls encompass tools and technologies such as password managers, firewalls, intrusion detection systems, and encryption.
- Administrative controls involve policies, procedures, and training programs designed to manage and govern an organization's overall security posture.

Technical security controls

Technical security controls are critical for safeguarding an organization's digital assets, including computer systems, networks, and data. These controls involve a range of technologies and practices designed to prevent, detect, and respond to cyber threats, including encryption, firewalls, access controls, antivirus, and malware detection. They are indispensable for protecting against cyber threats such as hacking, malware, and ransomware and ensuring the integrity and confidentiality of digital assets.

Password managers like Bitwarden provide reporting on password health, exposed or reused passwords, weak passwords, unsecured websites, inactive two-step logins, and known data breaches.

Administrative security controls

Administrative security controls are measures designed to manage and govern an organization's security posture through policies, procedures, and training. These controls are essential for guiding employee behavior and ensuring compliance with security standards. Administrative security controls are crucial for protecting against insider threats, social engineering, and compliance failures and for ensuring a comprehensive approach to security management.

- Clear guidelines around security policies and procedures help employees understand their roles and responsibilities in maintaining security, ensuring consistent application of security measures.
- Educating employees on security best practices and potential threats helps create a security-conscious culture and reduces the risk of human error.
- Incident response plans enable organizations to respond swiftly to security incidents, minimizing damage and ensuring a coordinated response.
- Adhering to compliance and regulatory requirements, such as HIPAA and PCI-DSS, ensures that organizations meet their legal obligations and protect sensitive information.
- Routinely identifying and mitigating security risks helps organizations avoid potential threats and maintain a robust security posture.

Get started with Bitwarden

Security controls are indispensable measures organizations must implement to protect their assets from a wide range of security risks and threats. Understanding the different types of security controls — physical, technical, and administrative — and their functions is crucial for developing an effective security strategy. Additionally, being aware of commonly overlooked areas, such as security awareness training and physical security controls, can help organizations address potential vulnerabilities. By adopting a comprehensive approach that includes a combination of these controls, organizations can ensure the confidentiality, integrity, and availability of their information and assets, thereby enhancing their overall security resilience.

You might also like:

Strengthen business IT security with best practices for 360° security