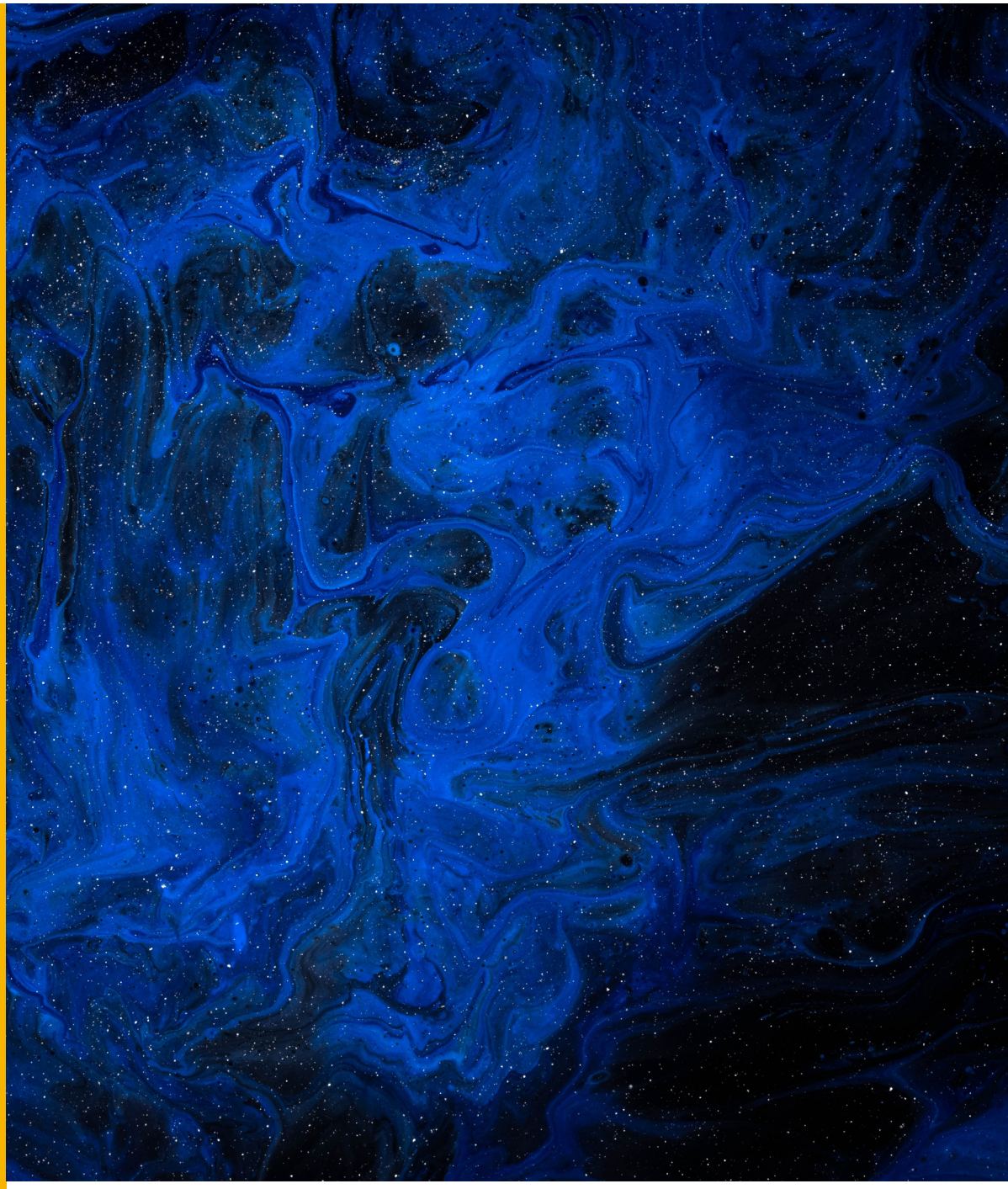
Petri IT Knowledgebase Resource
A BWW Media Group Brand

PETRI
WE GET IT



Petri Whitepaper
May 23, 2022

Cybersecurity vs IT Security – Taking Responsibility for Organizational Information Security

Sponsored by
Devolutions

Overview

Protecting IT assets and data from external and internal threats is complex. So when developing a security strategy, it's important to determine what threats an organization faces, what assets need to be protected, and who is responsible for what.

In this whitepaper, we will compare the differences and similarities between cybersecurity and IT security. We'll discuss the role of CIO (who oversees the process of establishing risk and making sure that the organization is adequately protected) and how the tools required by cybersecurity and IT security teams differ.

What is cybersecurity?

Cybersecurity is the application of controls, processes, and technologies to protect data and devices from cyberattacks. Cybersecurity is often an umbrella term that encompasses numerous ways to protect data, servers, and end-user computing. Ultimately, cybersecurity aims to reduce the overall risk of cyberattacks and protect against unauthorized exploitation of systems, networks, and technologies.

Cyber-crime costs organizations thousands of dollars each year and causes massive disruption to businesses. Each year, around half of all US and UK businesses have at least one security breach.

Altman Vilandrie & Company, a strategy consulting group, conducted a survey of 400 IT decision-makers in 19 industries. The survey found that 48% of companies in the US had experienced a security breach. And in the UK, a survey commissioned by the Department for Culture, Media and Sport (DCMS) found that the average UK business identified 998 security breaches in the last 12 months—and 13% of those businesses were breached daily.

IT security vs cybersecurity

IT security is a subset of the traditional security methods of red teams, blue teams, ethical walls, and penetration testing. But unlike cybersecurity, IT security refers to the protection of servers, networks, computers, and information, regardless of whether they are connected to a public network like the Internet.

IT security functions might include tasks like establishing a strong password policy for Windows Server Active Directory (AD) and providing secure access to network shares on a file server. While the term cybersecurity is newer, it covers a broader range of disciplines than IT security alone. Nevertheless, there is a considerable amount of overlap between IT security and cybersecurity.

Who is at risk?

It's important to note that it's not just large companies or financial organizations that can be affected by security threats. All types of organizations are at risk, regardless of size or industry. The reality is that it doesn't matter if an organization has 5 users, 500 users, or more. Organizations have an obligation to keep customer data, company data, and employee data safe and secure.

Ultimately, cybersecurity and IT security are a part of every organization's information security measures to protect computers, networks, and programs from unauthorized access.

Who is responsible for cyber and IT security?

A key aspect to understand is that each part of a business can be affected by security issues. The various ways of attacking businesses might affect departments differently, but all departments face problems—whether common or unique.

In a holistic view of the IT organization, there are teams that focus on network security aspects altogether. Such teams, for example, are responsible for firewalls, which allow only particular ports and protocols through to a specified port on an IP address or range of IP addresses.

In the domain of data storage, there might be a team that handles digital rights management (DRM) to ensure that information cannot be used outside of the organization, should there be a breach. This team classifies data according to sensitivity and necessity. They are also the first responders if data is leaked or stolen.

Then there are the actual data processing teams. Because they believe that the point where the data is processed is essential, they always encrypt data, and ensure that data is only accessed by the right people —either through privileged access or otherwise.

All these areas of expertise are important. But the weakest link in these areas isn't data, urgency, processing, or the network—it's the people themselves.

The role of Chief Information Officer (CIO)

As CIO, it's important to look at all the risks. These include understanding where the data is stored, whether it is encrypted, whether the data should be encrypted in transit, and what APIs are used to process the data.

IT security policy

Many businesses will have an IT Security Policy, and it's the staff's responsibility to attend the relevant training and adhere to policy and procedures. These policies may be specific to the workplace and the risks it faces. Different teams, different problems.

Employee understanding and awareness are key to protecting systems and data. It must be every employee's responsibility to keep information safe.

Beyond the network, services, and datacenter

By establishing a strong IT Security Policy, based on a risk assessment of the organization, IT can define what policies and procedures all employees must follow to keep data and systems secure.

Below are three important aspects of IT security that are usually included in an IT Security Policy document. These responsibilities are usually dealt with by IT security teams and not cybersecurity.

1. **Store data in sanctioned locations** – Storing organizational data in locations that are adequately protected, regardless of whether the data includes sensitive intellectual property or personally identifiable information (PII), is important for securing the future operation of any organization.

2. **Secure passwords** – Strong passwords must be enforced: it's a basic security measure. Weak passwords leave an open door to someone trying to access data and systems. A good or strong password contains a sequence of letters, numbers, or other characters—and the longer the sequence, the better.

   It's important to educate employees not to write down passwords, or to keep them in their phones or in a spreadsheet. Ultimately, if staff are struggling, they should be encouraged to use a password manager that provides a secure vault to manage all of the end user's business passwords in a single place.

3. **Privileged access management (PAM)**– Privileged access management is the process of managing and controlling access to privileged accounts. PAM is crucial in any organization, regardless of its size.

   PAM controls privileged user access to systems. A privileged user is someone who has an elevated level of access to a network, computer, system, or functionality, and who is authorized to perform functions that standard and elevated users are not authorized to carry out.

   Ultimately, PAM reduces threats to systems and data that users should no longer require access to. PAM uses identification and authentication controls to manage the risk of unauthorized access, then ensures the correct management of user accounts and auditing of their privileged access use.

   PAM policies should involve using a password vault and enforcing two-factor authentication. Ideally, a PAM solution should work natively with Active Directory (AD) and Office 365 to provide Role-Based Access Control (RBAC) to business systems without the overhead of creating new accounts in a separate system.

Reality of cybersecurity and IT security

While cybersecurity teams are busy with penetration testing, and while the blue team is defending the network from external threats, IT security professionals are responsible for the operational aspects of everyday security issues, like authenticating users and authorizing access to the IT assets required for employees to carry out their duties.

Evidently, the tools that IT security professionals need to fulfill their responsibilities in protecting the organization are different from those who are responsible for cybersecurity functions.

Security isn't just about plugging all the vulnerabilities and, in the process, also preventing employees from being productive. Cybersecurity and IT security solutions must not only work, but also allow end users to work. Often, we find ourselves in a restrictive state where we prevent an organization and its employees, including IT staff, from doing what they need to do for success.

Security and productivity shared a common goal: enhancing the organization. Where security and productivity meet is at the process level in designing a security strategy and operational integrations.

What does it all boil down to? Minimizing disruption to business. When the effects of a new process are too overwhelming for employees, ultimately security will fail. This failure creates a new vulnerability for the business: employees will try to find workarounds or other methods of getting work done.

Security solutions shouldn't be at odds with productivity. In fact, the data collected as part of a security effort should prove that security solutions facilitate productivity.

The stronger the security solution, the better insight we can provide and value for enhancing security, as well as any behavior analytics for productivity. The key is to drive adoption and understanding, as well as protect business services by preventing and prohibiting security breaches.

Conclusion

The world is moving forward from standard security processes, such as penetration testing and data encryption. However, the biggest risk to any business isn't the network, the servers, or the datacenter, but the staff employed.

Additional Information

For more detailed information about SMB cybersecurity challenges and solutions, be sure to check out Devolutions State of Cybersecurity in SMBs in the 2021 report.