FACTSHEET

Cloud security – managing risk and building resilience

Managing and mitigating risk is on the agenda of all businesses. The role of a security team is to identify, investigate and respond to threats to the business. Cloud security and cybersecurity are high on the list of threats that security teams need to manage.

Cloud security vs. cybersecurity

Cloud security is about the technology and processes used to safeguard the cloud environment against internal and external security threats such as unauthorized use. Cybersecurity is about protecting data, networks, and devices from cybercrime and unauthorized access that can damage business assets, revenue, and the organization's reputation.

Once security teams identify threats, they can then advise decision-makers so the business is empowered to make changes based on risk insights and security integration.

Managing risk

Operating a business comes with risks, but maintaining an acceptable level of risk is key. Risk maturity is a term used to explain the ability to prioritize so that high-risk issues are cost-effectively managed. Organizations that understand their appetite for risk and have an effective risk management framework are considered to have high risk maturity.

While cloud and cybersecurity attacks happen in a technical environment, they also represent a risk to the whole organization and should, therefore, be aligned to the risk mitigation framework, so they do not damage strategic business operations.

Aligning security risk management

Cloud and cybersecurity are not just technology problems. Security leaders must learn the importance of certain assets and data and be able to prioritize their team's time and budget to focus on high-priority issues and solutions.

Security leaders need to work alongside business leaders and build strong relationships between them and the different teams within the organization. Security risks and business opportunities are ever-changing, so the security team needs to invest constantly in building and maintaining these relationships.

Key to this is security teams understanding what is most important to the organization so they can understand how business value aligns with specific technical assets and the most important assets can be effectively protected.

How to get started

Security teams need to communicate in a language that business leaders understand so they can quantify the risk and impact on the organization's strategy.

They also need to actively listen to everyone across the business so they can understand the impact on the organization's services and information if they were to be compromised.

What security leaders learn from the relationships they build and their communication with business leaders can be translated into sustainable actions such as:

- Focusing on short-term priorities that deal with the most high-risk and business-critical issues, those immediate threats that could have the most detrimental impact on the organization.
- Protecting key assets and high-value data with suitable security controls that enable business productivity.
- Understanding and monitoring change to business priorities and strategies, so they stayed aligned.
- Set the direction for long-term priorities, so the overall security of the organization can be improved over time.
- Use a zero-trust strategy that assumes breach and allows dynamic risk-based decisions.
- Apply security best practices across the organizations, such as passwordless sign-in, multifactor authentication, and security patches.
- Retire old legacy systems that hinder productivity and invest in modern solutions that give your people time back to concentrate on high-value activities.
- Use role-based access control and data classifications to protect ata and limit the impact of a breach or attack.
- Develop a healthy security culture within the organization focusing on continuous learning, removing silos, knowledge sharing, and collaboration between security, IT, and all other teams and business leaders.

Understanding cloud and cybersecurity risk

According to Microsoft, when managing risk, it's important to understand the motivations and behavior patterns of the attackers.

Motivations

The motivations and incentives for different types of attackers are primarily based on financial gain or disrupting business processes to achieve a mission. Financial gain relates to criminal behavior that exploits data breaches with monetary value. Achieving a mission could be related to 'hacktivists' who want to disrupt the operations of a business that they believe to be damaging, for example, pharmaceutical organizations that test on animals.

Understanding the motivations of attackers helps organizations recognize what the potential impact of attacks might be, and security teams can focus their investments accordingly.

Behavior patterns

Depending on the motivation for an attack, organizations face a range of behaviors from their attackers. Financial gain attacks usually use inexpensive but effective tools and approaches that can be improved over time and can be scaled for high use. Mission-based attacks tend to be driven by long-term outcomes and are often well-funded.

Typical behaviors include:

- Being flexible and trying different methods and approaches that can be pivoted at speed.
- Being patient and taking time to understand and infiltrate technology environments.
- Stealth practices that look to hide evidence and tracks and lead security teams to look in the wrong direction.
- Using highly skilled and experienced people to gain access to data and remotely control systems.

Building business resilience

Security risk is an ever-present factor in business operations, and while the systems and data used can never be entirely safe, organizations can build their resilience to security attacks.

If security initiatives focus on increasing the resilience of business operations in the face of security attacks, risk can be reduced, and continuous improvements in how security responds to attacks are made.

Building resilience requires a zero-trust strategy that assumes a breach. It needs continuous investment across the full lifecycle of security risk.

Before an attack

Continuously seek to improve the organization's attitude to risk and its ability to respond to an attack. Most techniques are designed to raise the cost of attacks, forcing attackers to develop new methods and approaches that raise their costs and slow down their progress.

During an attack

Business continuity is essential, so ensuring operations can continue during an incident is key. Protecting business-critical operations should be the focus of all efforts. The secondary focus will be on understanding how the attackers gained access and then removing them from the environment.

After an attack

If operations have been damaged, then repairs must start immediately to restore full business operations. There also needs to be a focus on not allowing the same attack to occur again. Attackers learn from their endeavors, and so must the organization. Look at what was attempted or achieved and develop prevention strategies and barriers.

Security resilience goals

Security resiliency is about supporting the resiliency of the organization. It enables agility, adaptability, and innovation. It finds ways to allow business innovations and new technology adoption, so organizations are ready for anything. This was especially highlighted at the start of the pandemic when businesses had to quickly move to remote working. It is also focused on limiting the impact of disruptions caused by attacks.

Assume breach approach

Criminal attackers are constantly operating and trying to breach and compromise organizations. When security assumes breach, it works on a zero-trust principle that assumes breaches are always being attempted to ensure healthy security measures are taken all the time. This helps to prevent attacks, limits damage when they do occur, and allows organizations to recover more quickly.

Assuming breach drives changes across the organization and causes a shift in security culture and mindset that builds resilience and allows training, exercises, and different breach preparation activities to become the norm.

True resiliency requires close, continuously maintained, and nurtured relationships between security and business leaders.

Want to know more?

Visit this page to learn more about moving your Unit4 ERP to the cloud.

Click here

For more information, go to: unit4.com

UNIT4
In business for people