RAMPXchange

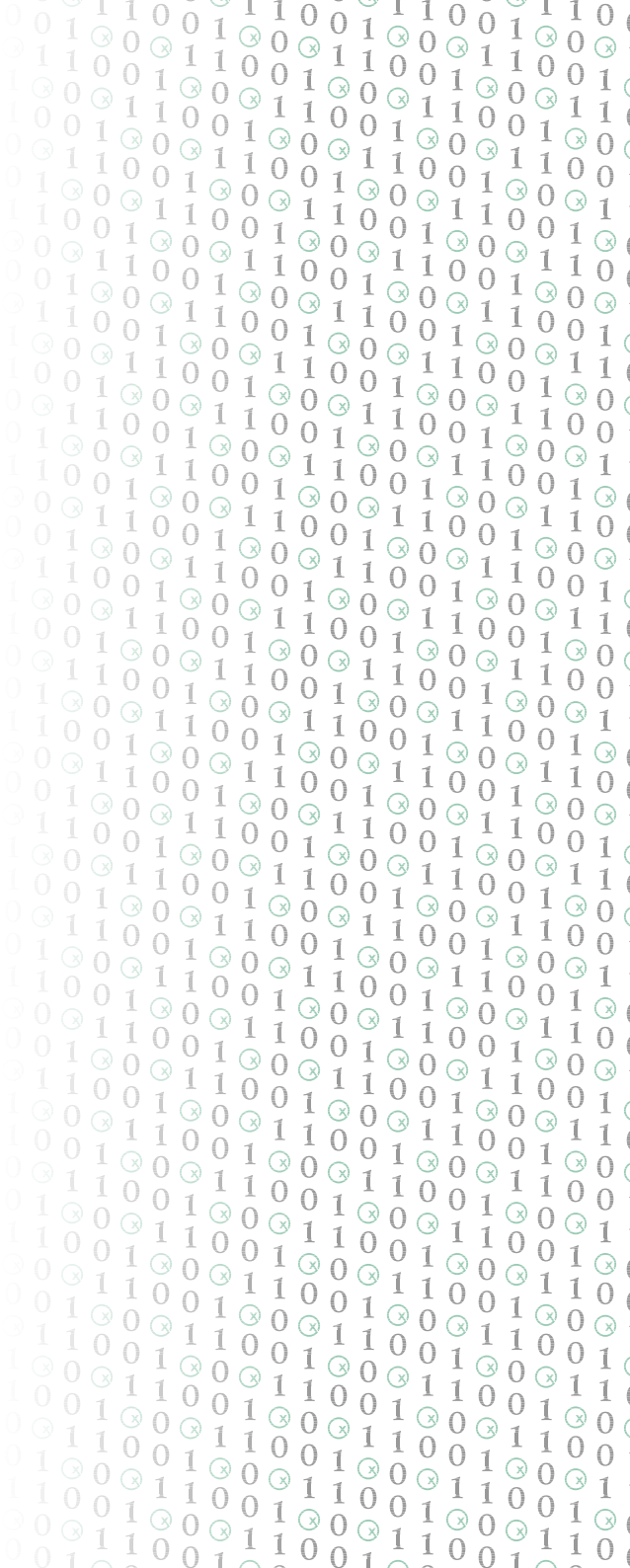
Creating a Culture of Cybersecurity Risk Management

rampxchange.com

Table of Contents

Part 1

Why You Should Create a Culture of Cybersecurity

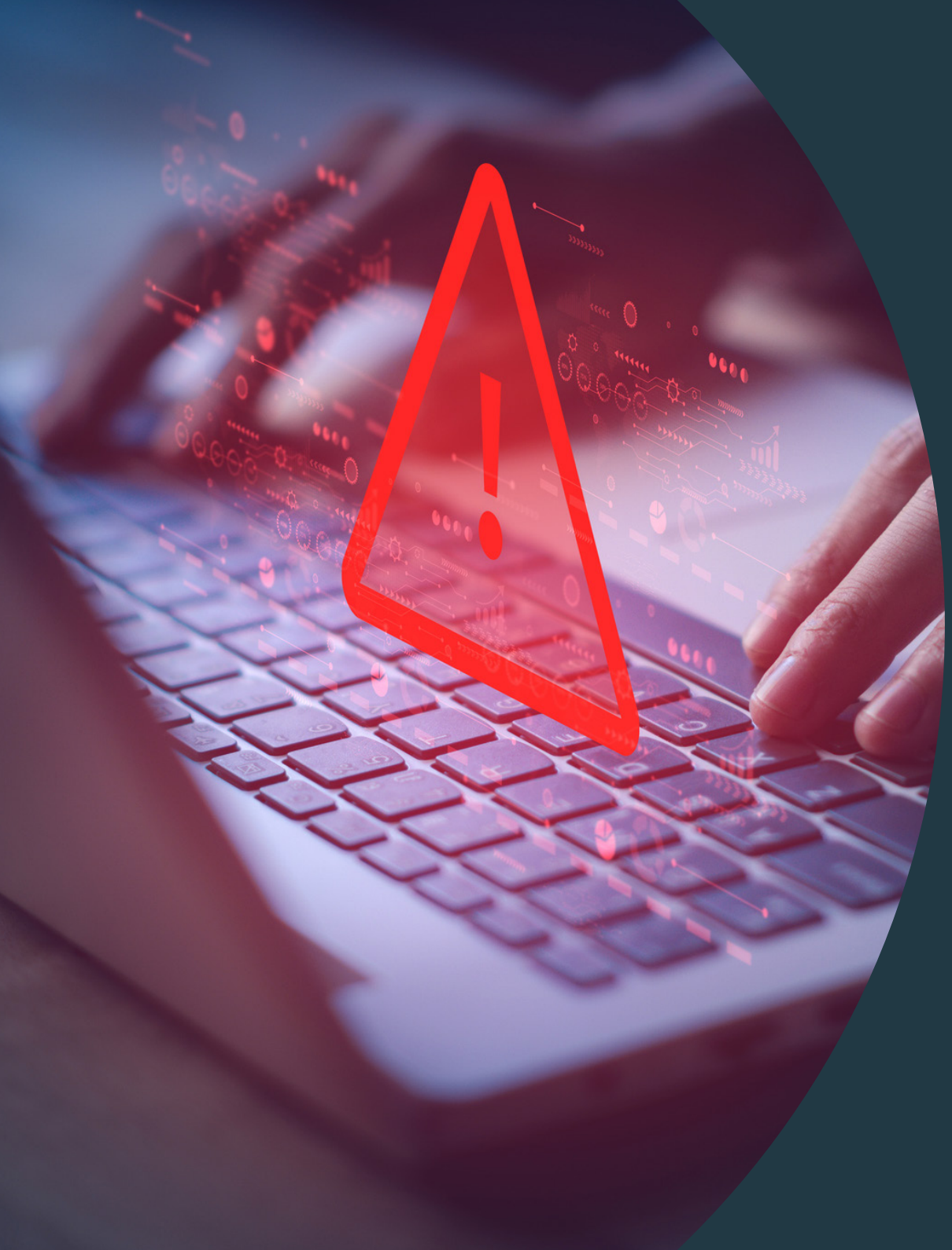


It Can Happen to Anyone

As a college intern in a mid-size corporate environment, Jeremy aimed to establish himself as a hard-working team player. Eager to impress, he responded promptly to an email he believed was from his department VP just before 5 p.m. on a Friday. In the email, the VP urgently requested Jeremy buy online gift cards for client meetings.

Jeremy complied, using a personal credit card as the VP assured him reimbursement on Monday. When Monday came with no word from his boss, Jeremy looked back at the email and realized it had come from a disguised domain. He had fallen victim to a phishing scam, a common tactic used by cybercriminals.

This experience serves as a powerful reminder of the crucial role of robust cybersecurity measures, particularly employee awareness training. Employees can learn to recognize and mitigate the risk of falling victim to phishing scams and other cyber threats through such training. By staying vigilant and verifying the legitimacy of requests, they can protect themselves and the company from potential harm.



The Cost of Cybercrime

Millions of instances of cybercrime go unreported every year. Of those officially reported to the FBI's Internet Crime Complaint Center (IC3), the losses amount to more than $27 billion from 2017 to 2022.

According to Ponemon Institute's **2023 IBM Cost of a Data Breach Report** research, phishing attacks and stolen or compromised employee login credentials are the two most common vectors for costly data breaches.

Cybersecurity Ventures and Cybercrime Magazine predict global cybercrime to cost the world **$8 trillion in 2023**. If it were its own country, cybercrime would be the world's third-largest economy behind the United States and China. The publication predicts costs could grow by 15 percent annually and reach $10.5 trillion by 2025, with ransomware alone costing victims **$265 billion annually by 2031**.

Additional Alarming Facts & Figures from the Report Include

$4.45 MILLION

Average worldwide cost of a breach

In 2023, the global average cost of a breach hit a record high, reaching $4.45 million. Specifically, breaches in critical infrastructure sectors such as financial services, industrial, technology, energy, transportation, communications, healthcare, education, and the public sector surpassed $5 million on average.

$9.48 MILLION

Average cost of a breach in the United States

Breaches in the United States cost an average of $9.48 million. Organizations that chose not to involve law enforcement in a ransomware attack experienced an average of $470,000 in additional costs. They also experienced a 33-day longer breach lifecycle.

ONLY ⅓

of breaches are identified by internal security teams

On average, organizations take over nine months to detect and handle a data breach. Only one-third of breaches are identified by internal security teams, while benign third parties or outsiders discover forty percent of breaches. Additionally, attackers disclose 27% of breaches as part of ransomware attacks. Breaches disclosed by attackers incur an average cost of 19.5% higher, equating to an additional $930,000, compared to breaches identified by organizations' internal security teams and tools.

Phishing Costs Major Companies Millions

The Anti-Phishing Working Group logged a record 4.7 million phishing attacks in 2022. While methods and attack surfaces have evolved, successful attacks often require little sophistication to swindle significant sums out of organizations ranging from small businesses to major corporations.

Three of the country's most expensive phishing attacks of record include:

Google & Facebook

Even two of the world's largest technology organizations have fallen victim to phishing scams. Over the course of three years, Google and Facebook were tricked out of more than $100 million. The cybercriminal posed as one of the companies' vendors, sending a series of fake invoices.

Beyond financial expenses, a cybersecurity incident such as a data breach can severely damage an organization's reputation and erode customer trust. News of a data breach or security breach can lead to negative media coverage, customer churn, and difficulty attracting new customers.

Ubiquiti Networks

A San Jose-based computer networking and wireless products corporation, Ubiquiti, lost almost $47 million in a phishing scam. Cybercriminals posing as the CEO and lawyers targeted the company's chief accounting officer, claiming a series of transfers were needed to close a secret acquisition. Only after the FBI issued a public service announcement did Ubiquiti discover it was one of the victims.

Upsher-Smith Laboratories

Cybercriminals targeted the accounts payable coordinator of Minnesota-based drug company Upsher-Smith Laboratories with a business email compromise (BEC) attack, impersonating its CEO with specific instructions for sending a series of wire transfers. While the company was able to recall one of the nine transfers, the cybercriminals made off with more than $39 million.

Recorded phishing attacks—4.7 million

Part 2

How to Create a Cybersecurity Risk Management Culture

How to Create a Cybersecurity Risk Management Culture

Cybersecurity culture refers to the collective company mindset, practices, and procedures that prioritize the protection of digital assets and infrastructure from cyber threats. It involves the technical measures and protocols and cultivating a security-conscious mindset among leadership and all employees.

Establishing a culture of cybersecurity does more than protect an organization's private data and sensitive information; it also plays a crucial role in attaining and maintaining customer trust and loyalty. Overall, cybersecurity culture encompasses a holistic approach to combat cyber threats, involving employee education, risk assessment, and proactive measures to minimize risk.

"We need a culture of cybersecurity because you can't tell everyone everything they need to do. You need them to understand that organizational safety is part of what they need to do in today's world."

-Keri Pearlson, Executive Director, Cybersecurity at MIT Sloan (CAMS)

Keys to Establishing a Strong Cybersecurity Culture

1.  Create a Company-wide Culture

2.  Communicate Clear Expectations Through Thorough Training

3.  Conduct Regular Testing & Evaluations

Create a Company-wide Culture

Leadership Level

Organizations with a mature cybersecurity posture reinforce their risk mitigation culture at every level, starting from the very top. Company leadership and executives can't expect employees to prioritize cybersecurity concerns if management doesn't lead by example. CEOs talk about security in all-hands meetings, and management clarifies to everyone that it's an intrinsic part of the company values. When proper cybersecurity behaviors are consistently demonstrated and reinforced by executives, including those who may not have an everyday primary focus involving security, it creates a stronger cybersecurity awareness throughout the organization.

Group Level

Cybersecurity topics and issues begin to permeate relevant discussions between employees and affect how they work together. Meetings include more discussion of cybersecurity-related topics, and even non-technical groups seek advice and guidance on operating more securely.

Group-level activities show that cybersecurity is important to the team, driving better and more secure behaviors and interactions daily. By integrating cybersecurity into an organization's culture and making it a shared responsibility, individuals become more vigilant and proactive in identifying and addressing potential security risks.

Individual Level

Employees gain a general, heightened awareness of possible threats and cyber incidents in everyday work. More importantly, they feel empowered to take individual action and know how to respond in the event of an incident.

Cybersecurity awareness permeates groups, divisions, and departments, ultimately influencing individuals' day-to-day actions. By integrating cybersecurity into an organization's culture and making it a shared responsibility, individuals become more vigilant and proactive in identifying and addressing potential security risks.

Communicate Clear Expectations Through Thorough Training

Communicating relevant information, policy changes, and expectations to all employees is crucial in establishing a strong cybersecurity culture. One of the primary goals of communicating cybersecurity information is to educate employees about potential threats the organization may face, such as phishing scams, malware, and social engineering tactics.

Outline the specific actions and behaviors expected of employees to safeguard sensitive information. For example, they may be required to update passwords regularly, use only secure networks, and report any suspicious activities to the appropriate channels. By clearly communicating these expectations, individuals can better understand their roles in maintaining a secure environment and productive cybersecurity culture.

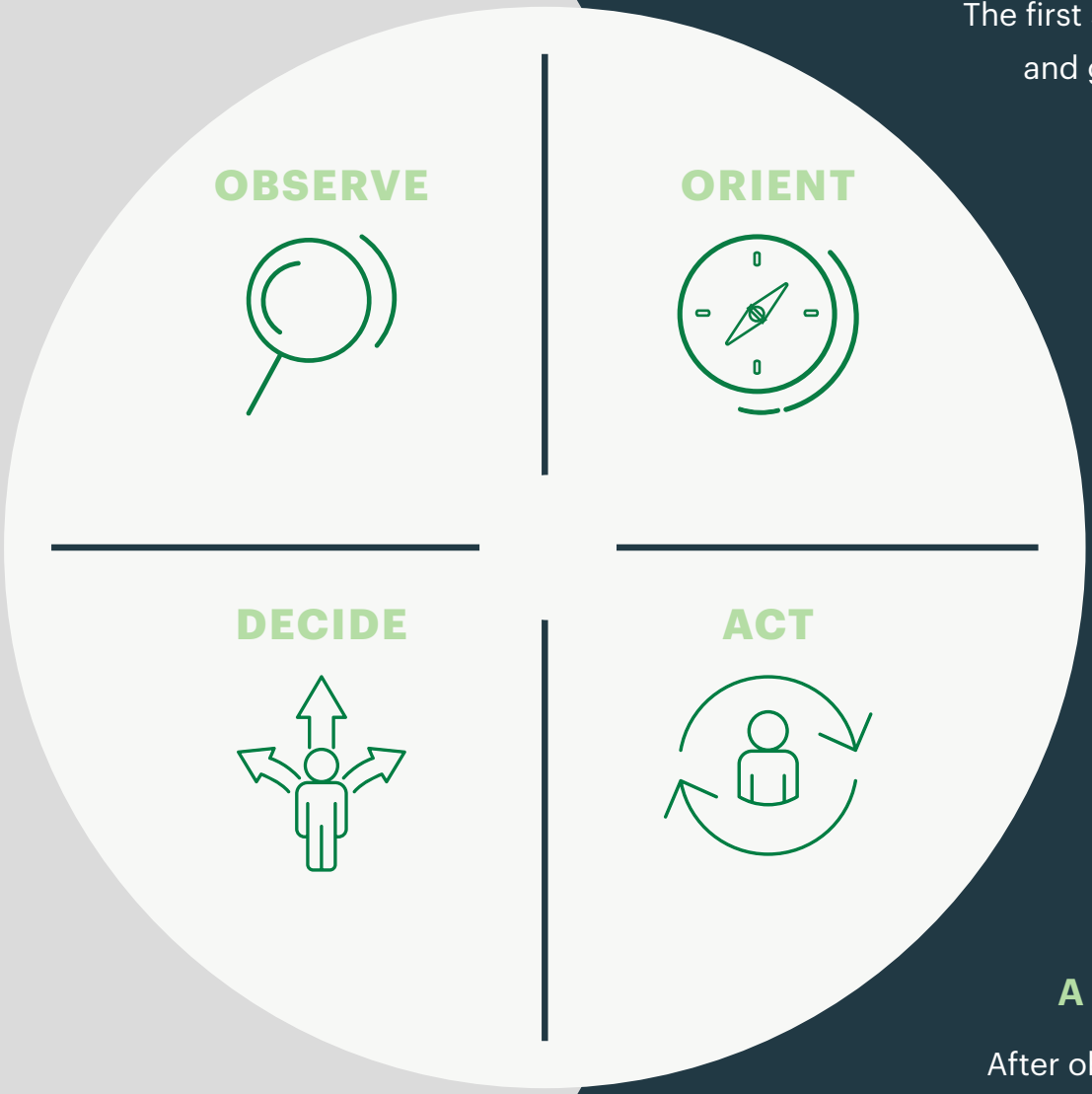
Cybersecurity training isn't a "one-and-done" exercise. New threats, such as phishing tactics and other sophisticated techniques, can emerge and evolve rapidly. Regularly review and update organizational security policies, setting aside time to review them with employees. Onboarding new personnel, including interns or temporary hires, should always include cybersecurity training.

Conduct Regular Testing & Evaluations

In addition to consistent updates from leadership or a designated cybersecurity culture executive, organizations and employees can benefit from exercises that test cybersecurity incident awareness and readiness capabilities.

Simulations that mimic real-world phishing attacks or social engineering tactics help individuals stay vigilant and recognize what should happen in the event of an actual cybersecurity incident. Create simulations that are specifically targeted to users with varying levels of experience and departments. After drills, follow up with employees to field questions and give them feedback on how their responses would have affected the organization in the event of an actual attack.

Consider training with tools such as the OODA loop. The OODA loop is a decision-making strategy designed to help individuals quickly take all available information into context and make the most appropriate decision within a high-stakes or volatile scenario. While initially developed for training soldiers to make time-sensitive decisions, it's a thought process that can help team members assess the situation, respond appropriately, and refine practices to prepare for future similar instances.



O – Observe

The first step is identifying the threat, gathering data, and gaining an understanding of the situation.

O – Orient

The orientation phase involves reflecting on what's been found in observation and unbiasedly identifying potential outcomes. This step requires a significant level of situational awareness.

D – Decide

Considering the potential outcomes and results, the decision phase proposes the best course of action and a robust response plan.

A – Act

After observing, orienting, and deciding, acting is the final step of implementing the actions.

Part 3

Know Your Suppliers

Assessing the Cybersecurity of Potential Partners & Providers

As organizations run more of their workloads and operations in cloud environments, they benefit from expanding their reach and capabilities. At the same time, it also increases their risk exposure.

Cloud environments are frequent targets of cybercriminals. According to the **2023 IBM Cost of a Breach Report**, 82% of breaches involve data stored in the cloud in public, private, and multiple environments. Thirty-nine percent of those cloud data breaches involved data that is stored across multiple environments.

It's become increasingly unlikely, if not impossible, for any organization to maintain every facet of its digital infrastructure and workflows on its own. Therefore, organizations must partner with providers, vendors, and suppliers who share their commitment to a strong cybersecurity posture.

Seven Critical Factors for Assessment

Because of these inherent risks related to cloud operations and software-as-a-service (SaaS) solutions, there are several critical factors organizations must consider when in the market for a potential partner and service provider:

1 Transparency

Transparency builds trust and helps organizations confidently assess the cybersecurity capabilities of prospective or existing providers. A secure provider should be transparent about its cybersecurity practices. They should be willing to provide information detailing their security controls, complete audit trails, response plans, and more.

Seek out providers and partners that proactively offer transparency reports, independent audits, incident overviews, and service agreements that clearly define their and your security commitments.

2 Reputation: What's Their Track Record?

Begin with thorough research into the provider's reputation by seeking out reviews, ratings, or testimonials from existing customers. While a track record of positive feedback doesn't necessarily mean a provider's solutions are ironclad, it can indicate the company's commitment to its customers.

Using search engines and news aggregators to gather relevant information, look for news articles, press releases, or reports that mention any security incidents or breaches related to the provider. Additionally, check databases that track and catalog security breaches across various industries, such as the Open Security Foundation's DataLossDB or the Privacy Rights Clearinghouse's Chronology of Data Breaches.

Seven Critical Factors for Assessment

3 Certifications, Standards Compliance, & Independently Assessed Controls

Assess whether the prospective provider has earned any reputable security certifications or has undergone independent audits of their security controls.

Reputable cybersecurity standards and cloud security certifications for cloud service providers include ISO-27001, the NIST frameworks (NIST RMF & NIST CSF), SOC 2, FedRAMP, and StateRAMP.

Complying with these standards and maintaining relevant certifications demonstrates the provider's commitment to widely recognized and respected cybersecurity practices.

4 Capable Data Encryption

Encrypting data is a fundamental cybersecurity measure for protecting sensitive information from unauthorized access. Strong encryption ensures that even if a major breach occurs, the stolen data will remain unreadable and unusable to cybercriminals.

Ask about a provider's approach to encrypting data in transit and at rest. They should use strong encryption algorithms such as AES-256 to protect stored data at rest. Furthermore, encryption should apply to all storage systems, including databases, file systems, and backups. For in-transit data (between your organization and the provider's infrastructure), look for strong protocols for encryption, such as transport layer security (TLS).

Seven Critical Factors for Assessment

5 Access Controls & Identity Management

The growing use of cloud platforms has provided many companies' employees with expanded opportunities to work remotely from anywhere. However, the benefits also introduce new challenges that can increase the likelihood of theft or other malicious intent.

Effective cloud security is only as strong as any cybersecurity infrastructure's gatekeeping abilities. Robust access controls and identity management measures are critical to prevent unauthorized access to sensitive systems and private data.

They should maintain detailed logs of user access and activities, which can be helpful for monitoring and investigating potential security incidents. Ask whether the provider provides access to these logs or if they offer log management solutions.

6 Physical Security

Secure cloud storage is critical, but providers must also prioritize their physical security measures. Ask for information regarding the physical security safeguards in place to protect data centers and server locations.

Minimum measures should include access controls, security personnel, video surveillance, redundant power supplies, and climate-control systems to minimize the risk of physical breaches or service disruptions.

Check whether the provider complies with industry standards related to physical security. For example, certifications such as ISO 27001 or SSAE 18 (SOC 1, SOC 2) indicate the provider has implemented appropriate physical security controls.

Seven Critical Factors for Assessment

7 Incident Response & Recovery

Even when using secure providers, data breaches can still occur. It's crucial to define both parties' roles in data backup and recovery in initial agreements, along with detailed response plans.

Inquire about the provider's security monitoring, including IDPS, CSPM, and SIEM tools, to ensure they can detect and respond to threats effectively. Understand their breach notification process, how they'll inform you of incidents, and their actions to secure your data if it's compromised.

Questions for Your Vendors & Third-Party Providers

Cloud services and evolving "as-a-service" solutions offer organizations a new world of exciting possibilities, but third-party suppliers are one of the biggest sources of data breaches. When identifying third-party providers for cloud services, including software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS), and function as a service (FaaS) solutions, organizations should keep five areas of consideration top of mind and ask the following questions regarding alignment with internal cybersecurity standards.

Vendor Risk Management

What is the provider's own internal cybersecurity posture—do they have a strong track record and reputation for effective security?

Are third-party assessments or independent audits of the provider's security controls available?

What happens to data if the provider experiences a security breach or goes out of business during the duration of a service contract?

Security Configurations & Management

Can specific settings and policies be configured to align with your organization's security standards?

How often is the underlying infrastructure updated and patched to address cybersecurity vulnerabilities?

Does the provider offer transparency and the tools necessary for monitoring and auditing cybersecurity events?

Identity & Access Management

Can the provider's solution integrate with existing identity management systems?

Are robust access controls available, such as multi-factor authentication or assigning permissions based on users' roles and necessary levels of access?

Incident Response & Compliance

What is the provider's incident response strategy, and how does it align with your organization's response and recovery efforts?

Is all activity within the cloud environment monitored and logged?

Can you easily generate compliance reports?

Data Security & Privacy

How is data encrypted at rest and in transit, and with what encryption standards?

What measures are in place to prevent unauthorized access to data by both external attackers and internal users?

Has the provider achieved compliance with frameworks or regulations relevant to your industry, such as GDPR, NIST, HIPAA, or SOC 2?

Part 4

Reducing the Burden on Internal Resources

Leveraging Third-Party Validations for Streamlined Cybersecurity Compliance

The Challenge of Self-Attestation

Self-attestation has been a common approach in which organizations internally assess and declare their cybersecurity compliance. While it provides a degree of flexibility, it often comes with various challenges and limitations.

Resource Intensiveness

Internal assessments require significant time, expertise, and financial resources, which can strain an organization's workforce and budget.

Subjectivity

Self-assessments are susceptible to inherent bias, as organizations may purposefully downplay or inadvertently overlook vulnerabilities and non-compliance issues.

Inconsistency

Standards and practices can vary between organizations, leading to inconsistent cybersecurity postures and challenges for benchmarking or comparing security levels.

Lack of Credibility

Self-attestation may not be wholly trusted by clients, partners, or regulatory bodies, leading to potential difficulties in business relationships and regulatory compliance.

Organizations face a growing need to ensure robust cybersecurity practices in today's digital landscape. However, achieving and maintaining a strong cybersecurity posture can be resource-intensive and burdensome for many organizations.

The Role of Third-Party Validation Programs

Third-party validation programs like FedRAMP and StateRAMP offer a compelling solution to these challenges and can benefit organizations in many ways.

Objective Assessments

Independent, third-party assessors with cybersecurity expertise conduct comprehensive evaluations. These assessments are objective and follow standardized criteria, reducing the risks of any bias or subjectivity.

Resource Efficiency

Organizations can leverage the expertise of assessors, reducing the burden on internal resources while achieving cost savings and valuable efficiency gains.

Benchmarking & Consistency

Third-party validation programs establish consistent benchmarks and standards, allowing organizations to measure their cybersecurity posture against a recognized baseline, relevant industry standards, and widely accepted best practices.

Enhanced Credibility

Certifications from reputable third–party programs significantly enhance an organization's credibility and can be valuable in building trust with clients, partners, and relevant regulatory bodies.

Regulatory Compliance

For organizations subject to specific regulatory requirements, third-party certifications can simplify compliance by demonstrating adherence to established standards.

Choosing the Right Program for Your Organization

The free market offers a vast plethora of cybersecurity products and solutions, allowing municipalities, public entities, and businesses of all sizes to choose solutions best suited to their needs. By opting for and leveraging third-party assessments, organizations can reduce the burdens on their internal resources, better manage risk, and build a culture of cybersecurity that stands up to the ever-evolving threat landscape. When considering a third-party validation program, organizations should assess their specific needs, compliance requirements, and the nature of their operations. It's essential to choose a program that aligns with their goals and industry standards.

FedRAMP

FedRAMP is designed for federal agencies and their cloud service providers. It streamlines the authorization process, ensuring that cloud solutions meet the stringent cybersecurity requirements set by federal agencies. This is particularly valuable because federal agencies handle a vast amount of sensitive and classified data, making the security of cloud solutions a top priority.

For organizations serving federal agencies or those looking to provide cloud services to the government, FedRAMP offers significant cost savings. Rather than each agency conducting its own assessments and authorizations, FedRAMP provides a standardized, government-wide approach. This minimizes redundancy, cuts down on assessment times, and reduces the financial burden on CSPs. It allows CSPs to focus on developing secure cloud solutions and serving their government clients more effectively.

FedRAMP certification is a gold standard for cybersecurity in the federal sector. It ensures that CSPs have implemented strong security controls and practices, making them a trusted choice for federal agencies. By adhering to FedRAMP standards, CSPs not only meet the immediate requirements but also significantly enhance their security posture, attracting other clients and partners who value robust cybersecurity practices.

StateRAMP

StateRAMP is an essential program designed to extend the benefits of third-party validation to state and local governments. Recognizing that state and local governments handle a significant amount of sensitive data, StateRAMP addresses the unique cybersecurity needs of these entities. It helps them meet cybersecurity standards and protect critical information while facilitating collaboration and interoperability across different jurisdictions.

State and local governments often face resource constraints and may lack the cybersecurity expertise needed to ensure their systems are adequately protected. StateRAMP addresses this challenge by providing a structured framework and assessment process, allowing governments to leverage the expertise of independent assessors, relieving the burden on their internal resources and budgets.

StateRAMP participation benefits private sector businesses and organizations looking to do work with state and local governments in several significant ways. The program's streamlined and standardized framework and leveraging of third-party assessors saves time, money, and resources that would otherwise be wasted navigating a patchwork of paperwork and different standards or requirements across various jurisdictions.

Adhering to StateRAMP standards helps businesses enhance their cybersecurity posture, ensuring security controls and practices are robust and resilient to the digital landscape's emerging cyber threats. Obtaining StateRAMP certification gives potential vendors and partners a significant competitive advantage during requests for proposals and bidding on state or local government contracts.

Interoperability is a critical aspect of StateRAMP. It ensures that state and local governments can share information and resources effectively while maintaining a consistent cybersecurity standard. This is particularly important in the context of disaster response, law enforcement, and public health, where timely and secure data sharing can be a matter of life and death.

By participating in StateRAMP, state and local governments signal their commitment to cybersecurity. This fosters trust among citizens, businesses, and federal partners. It also encourages collaboration between government agencies and the private sector as businesses seek to work with governments that prioritize cybersecurity. Additionally, it can make grant applications more competitive, as funders are increasingly requiring compliance with cybersecurity standards.

Learn more about the benefits of StateRAMP

Find Solutions in RAMPxchange

The cybersecurity world must band together in response, creating a collaborative ecosystem where the free market builds a robust network of cybersecurity defenders.

Introducing RAMPxchange, a dynamic marketplace where the forces of the free market fortify the defenses of organizations across the globe. Here, cybersecurity professionals, firms, and independent experts can come together to offer their skills, knowledge, and services in a unified effort to protect against cyber threats.

By tapping into the marketplace, organizations can:

- Access the expertise of cybersecurity professionals on an as-needed basis.
- Source solutions tailored to their unique requirements.
- Stay ahead of emerging threats with the latest threat intelligence.
- Collaborate with specialists in specific areas of cybersecurity.

Learn more about RAMPxchange

About RAMPxchange

After going through the FedRAMP process and helping found StateRAMP, Knowledge Services ownership learned a lot. RAMPxchange is a result of the ownership's desire to share what they learned to make it easier for public and private organizations to work together. We strive to bring efficiency, transparency, simplification, and cost savings to everyone wanting to improve the cybersecurity posture of our nation.

Our Values

Community

In our knowledge-based economy, the sharing of information is paramount. We rely on each other to communicate and gain strength from our different experiences.

Protection

Technology changes at a rapid pace, and people's lives are affected every day by cyber attacks. Improving cybersecurity for all is about protecting and serving people.

Integrity

In business and in life, we believe honesty is always the best policy. We take pride in our integrity and in doing what's best for the people we serve.

Innovation

Amidst a wave of transformation, we embrace opportunities to create, scale, and elevate our craft. We're empowered by the prospect of making organizations more open and collaborative.

Final Thoughts

In the ongoing battle against cyber threats, the need for a united front has never been more apparent. The invisible war in the digital realm rages on, with cybercriminals constantly innovating and evolving their tactics. The cybersecurity world must band together in response, creating a collaborative ecosystem where the free market builds a robust network of cybersecurity defenders.

Contact us to learn more about the RAMPxchange marketplace, its members and how these experts can help you on your journey.

rampxchange.com/contact/