THE WESTWIND WATCH
Keeping Pace with Technology

WESTWIND

How To Prep Your Cybersecurity Efforts for 2022

Introduction

The Covid-19 pandemic and the subsequent rise in remote work arrangements was a brutal wake-up call for many businesses across the globe. The attempt by most organizations to simultaneously provide employees with secure access to on-premise networks/data while allowing for device flexibility exposed security flaws in legacy processes and systems.

With the shock of the Colonial Pipeline and near-disastrous Florida water hacks still reverberating, the question C-suite executives and business owners ask is…Are we ready for what cybersecurity will become? The reality is that cybersecurity isn't a destination or a milestone to be achieved, but rather a continuous journey.

Navigating this uncertain terrain requires organizations to develop and implement an agile cybersecurity strategy…and the foundation of such a strategy lies in designing repeatable cybersecurity processes. But first, business leaders must determine their risk tolerance, i.e. how much risk their organization is willing to handle. Doing so will enable them to establish the right priorities to determine what to protect and how to protect it.

Cybersecurity comes with a cost and the ROI isn't always visible. Cybersecurity efforts are preventative by nature which makes it challenging for some organizations to effectively budget time and resources for cybersecurity initiatives. They either don't do enough or end up going overboard by deploying a plethora of siloed products.

As we approach 2022, there's a greater need for robust, flexible, and sustainable security measures to protect data and networks from the increasingly insidious and sophisticated hacks of criminals.

To help CIOs and IT leaders improve cybersecurity hygiene, find new ways to protect the company from current cyber threats, and ensure their company remains protected, here are some recommendations on how to prep your cybersecurity efforts for 2022.

There's no such thing as a 100% secure network or database based on factors such as the constant evolution of the threat landscape, the challenge of training all your employees to be perfect at detecting phishing attempts 100% of the time, and the ongoing, iterative nature of cybersecurity.

Develop a Robust Cybersecurity Incident Response Plan

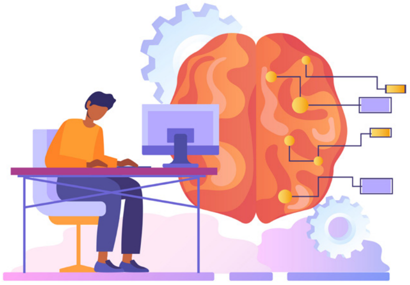
It all starts now. Simply put, an ounce of prevention is far more valuable than a pound of rectification. Organizations need to start prepping their strategies to lay a strong and sustainable foundation for securing their data and networks in 2022.

The 2020 Ponemon Institute's Cost of a Data Breach Report compared companies that developed a cybersecurity incident response plan (CSIRP), tested said plan via simulations and tabletop exercises, and designated an incident response (IR) team with those that took no such measures. The report found that the former saved an average of $2 million in data breach costs compared to the latter.

The future of cybersecurity requires teams to move beyond static incident response strategies designed to mitigate previously successful threat vectors, and test out methodologies that are flexible enough to tackle the threats of tomorrow. Since today's hackers are evolving their strategies, security teams must do the same to stay ahead.

Not only is there an explosion of ransomware with ransom demands, but hackers are also integrating new data theft-based extortion tactics into their exploits. While breaching systems and networks, they also steal sensitive business information and threaten to release it publicly if their ransom demands aren't met.

To keep pace with these and other such tactics, organizations must revise enterprise-wide incident response and crisis recovery plans to keep pace.



Expand Security Products to Include Artificial Intelligence

As hackers develop increasingly sophisticated malware and look for unprotected attack vectors to deploy automated cyberattacks, many organizations are turning to AI-powered cybersecurity controls to protect their data assets.

AI can be used either defensively or offensively to detect and mitigate the impact of breach attempts. For instance, AI-powered threat intelligence can help organizations reduce incident response times by anticipating future attacks via pattern recognition in historical data. AI helps to analyze the thousands of alerts and identify those that are most likely to signal actual threats.

This is dissimilar to traditional cybersecurity techniques that use indicators or signatures to identify threats…a method that works about 90% of the time and only intercepts known threats. Integrating AI-powered cybersecurity controls enables organizations to increase detection accuracy and also helps intercept unforeseen threats. As such, expanding your cybersecurity assets to include AI-powered solutions is a great way to prep your organization for the future of cybersecurity.

Review Existing Investments in Cybersecurity Products

It's no surprise that organizations are increasing their investment in cybersecurity. Sixty-six percent of respondents to an Enterprise Strategy Group (ESG) survey said that their organizations had plans to increase their cybersecurity spending in 2021. And from all likely indications, this trend will continue into 2022.

However, more spending isn't necessarily better. The key is to make intelligent, strategic investments that facilitate the thorough protection of network and data assets. Savvy organizations are reviewing their existing security products to identify redundancies and free up their budget by reducing the number of security products they use.

Rather than purchasing and deploying numerous security products, you can do more with less by identifying a holistic security product that provides optimal protection for your IT estate while keeping to budget considerations and organizational goals.

Also, business leaders should evaluate existing hardware and upgrade where necessary. Even a well-designed cybersecurity strategy can be undone by an overlooked vulnerability or a single point of failure. Most cybersecurity teams need to contend with:

- Budget, staffing, and resource limitations
- Lack of proper security awareness and culture among users
- Use of AI and ML technologies to automate exploit breach attempt
- New security vulnerabilities due to the expansion of cloud solutions and the IoT
- Increased attack surfaces and vectors propelled by the growth in data volumes and remote workers

To cope with the continually evolving threats and prep their organizations for the future, cybersecurity teams need access to the latest tools, solutions, and processes.

In addition to robust tools for penetration testing, vulnerability scanning, intrusion prevention, network security monitoring, data encryption, virtual private networks (VPNs), etc., you should also consider adding the following to your cybersecurity arsenal:

- Multifactor authentication protocols.
- Tokenization of sensitive business data to prevent exposure in the event of a successful breach.
- Zero trust security solutions that enforce stringent authentication requirements for devices and users.
- Unique tools for user behavior monitoring, data loss prevention, and endpoint management and protection.
- Secure Access Service Edge (SASE)

SASE is a network architecture that acts as a gatekeeper of sorts for corporate networks - it identifies devices and users, applies policy-based cybersecurity measures, and provides secure access to authenticated users and applications. This helps organizations provide uninterrupted secure access to their users, irrespective of location or device. Leveraging SASE is a great way to increases security for organizations with remote workforces.

Review of OPEX vs. CAPEX Expense Structures Around Cybersecurity Products

The debate concerning whether cybersecurity spending should be an ongoing operating expense or a one-time capital expense has been ongoing for quite some time. As CISOs attempt to cost-justify the deployment of new cybersecurity products, the question of using OPEX vs CAPEX expense structures has become central.

In previous years, cybersecurity spending was more likely to be a CAPEX rather than an OPEX item. But with the supply chain disruptions and the subsequent economic realities of the pandemic reducing company cash flow (and by extension, budget considerations), most organizations are leaning towards deploying cybersecurity products via the "As a Service" model.

To get the best value for their cybersecurity budget, a lot of companies are transitioning to an OPEX model. The CAPEX method makes no room for the depreciation and obsolescence of security products as technology advances and threat actors evolve.

Embracing the Security as a Service or subscription consumption model allows companies to enjoy the latest cybersecurity product and expertise by paying a monthly or quarterly fee...and this doesn't fit in with the CAPEX model. The OPEX model is a win-win for everyone since service providers enjoy greater ROI from building Recurring Monthly Revenue (RMR) while organizations enjoy greater value from paying a subscription fee for top-notch protection.

Also, it seamlessly fits in with the Software as a Service model, which businesses and individuals have been using for a long time now to spread out the cost of acquiring over a long period, while gaining greater flexibility, improving scalability, and it can help prevent vendor lock in.

This also improves the accessibility of security products to all enterprises, regardless of size, seasonality, or growth- from mom and pop operations to Fortune 100 companies.

Improve Response to Successful Breaches

While many organizations focus all their efforts on preventing breaches, very few actually plan for what would happen in the event of a successful attack. If a breach does occur, it's very important that your security team quickly understands the nature of the attack, how and where it occurred, and what is at risk (services, data, systems). This will enable cybersecurity experts to execute the appropriate mitigation actions to reduce the impact of the breach on business activities.

Regardless of how resilient your threat prevention plans are, it's in your best interests to develop a solid breach response plan. Such a plan should include the following:

- Clearly define roles and responsibilities of all personnel involved in the response plan
- Design a risk assessment strategy and detail various alert levels to designate the seriousness of incidents
- Instigate emergency backup plans to ensure business continuity in the event of a successful breach
- Organize regular awareness training programs to prepare employees for incident response situations
- Test overall preparedness of your organization by simulating attack scenarios
- After a successful breach (or simulation), assess the effectiveness of the response plan to identify loopholes and opportunities for improvements

Organizations without an incident response plan can leverage the services of managed security providers to develop and implement a customized response plan. Such tailored plans are more effective at limiting the damage and reducing the impact of a successful breach on operations, data, reputation, customer trust and revenue losses.

Organize Internal Cybersecurity Awareness Programs for Company Employees

Most business leaders know that there are gaps between the desired and actual cybersecurity culture within their organization. But, closing this gap is key to prepping the entire organization for cybersecurity into 2022 and beyond, especially since more and more threats target employees.

In the past, security awareness training was an event or a one-time thing. Now, smart organizations and CISOs recognize the impact of ongoing cybersecurity awareness training programs on employees and the role these programs play in an effective cybersecurity strategy.

Rather than organize seminars where rules and static policies are passed along to employees, awareness training now features interactive lessons that are tailored and personalized to individual employees.

These lessons form part of an informative approach that makes it easy for employees to imbibe a wholesome culture where security becomes automatic and plays a key role in the execution of daily tasks.

Furthermore, regular cybersecurity training initiatives help give employees a sense of belonging and inclusive feeling of being part of the overall cybersecurity strategy. It also provides each employee the opportunity to take ownership of the cybersecurity threat prevention efforts. Consequently, employees know that their actions will ultimately help the organization increase the resilience of its cybersecurity posture.

The current informative approach to cybersecurity awareness trainings can feature a mix of ongoing learning initiatives and regularly scheduled events interwoven with diverse approaches to suit a variety of learning styles. This makes it easier to instill a touch security mindset in employees at all levels of the organization.

To test the efficacy of these programs, cybersecurity leaders can run attack simulations and impromptu email phishing campaigns to promote vigilance and identify areas for improvement. They can also keep employees up-to-date on the evolving threat landscape, company-mandated security policies in response to emerging security issues, and possible attack vectors, by sharing content through relevant channels.

In addition, business leaders can develop content tailored to specific roles to better equip and engage employees and improve the organization's overall security posture. For instance, work with in-house developers to educate them on secure coding best practices, the latest vulnerabilities, and how to introduce security early into their development cycles.

Also, you can work with payment specialists and accountants to help them understand how malicious actors use phishing attacks, compromised emails, and other social engineering tactics to run payment scams.

Awareness training programs for employees aren't an item to be checked off a list but a process of continuous engagement that lasts for as long as cybersecurity remains a concern. In fact, savvy organizations are taking steps to modernize their security training in line with improving awareness around the increased risks associated with the massive push for remote work setups and the effects of the COVID-19 pandemic. Some of these steps include:

- Tailoring training to specific roles and responsibilities.
- Investing adequately in cybersecurity training and employee awareness initiatives.
- Identifying employee roles with the highest risk and prioritizing training efforts to get the best value.
- Testing effectiveness by monitoring the impact of awareness campaigns and identifying areas for improvement.
- Increasing awareness campaign effectiveness by personalizing training.
- Identifying ambassadors and volunteers within the workforce and leveraging their influence to improve cybersecurity awareness among their peers.
- Simplifying training content and process to ensure that every employee gets the messag.
- Using gamification and other techniques to make awareness training engaging and fun.
- Ensuring that senior management participates actively in all awareness campaigns. This motivates middle management and frontline workers to participate actively and adopt/implement security best practices.

Partner with Experts

A popular myth is that deploying more security products equals more protection. Effective cybersecurity isn't about spending tons of money to purchase every security tool in the market. It's more about aligning business priorities and the existential threat landscape with effective solutions.

With expert guidance, businesses can identify the approach, methodologies, and products to deploy to ensure the best value for their cybersecurity spend. They can benefit from:

- Less operational costs and oversight as a result of reduced technology sprawl.
- Stronger security due to more visibility and increased agility for threat response.
- Lower purchasing, maintenance, and overhead cybersecurity costs.

Having access to the leading-edge technology, scalable resources, and top-notch cybersecurity skills and expertise can make the difference between an average and an effective cybersecurity strategy in 2022. Partnering with experts can maximize the value of your cybersecurity spend, reduce overall costs, and allow you to achieve organizational goals.

Wrapping Up

Effective cybersecurity has become very crucial with the rapid expansion of remote work setups, cloud computing, and digital transformation initiatives. These trends are inadvertently increasing vulnerabilities and exposing new attack vectors which malicious attackers can take advantage of to damage business reputation, stop business operations, and inflict harsh ransom demands.

Staying ahead of today's attackers and prepping for the future of cybersecurity requires a three-pronged approach:

- Intelligent assessment and in-depth analysis of vulnerable IT assets to design a defense strategy.
- Comprehensive network and endpoint security,
- Proactive response plan to ensure business continuity in the event of a successful breach.

Approaching cybersecurity as an investment opportunity rather than a necessary evil can bring the entire organization together and allow them to proactively assess risk and protect its valuable data and resources.

(866) 345-4720 I wwcpinc.com

ABOUT WESTWIND

For over 25 years Westwind has supported medium to enterprise businesses locally and nationwide, no matter the industry. Our certified IT professionals help your business navigate the ever-changing tech landscape. Our network of cutting-edge partners allows us to provide the right solutions to meet our customer's specific needs – from hardware to software, workstations to training centers, auditoriums to secure data centers. With the latest in training and technology, Westwind is your partner for IT products, services and, of course, cyber security.

WESTWIND