INSIGHTS PAPER

Bulletproof your networks

Avoid risk, data loss and exposure from security breaches.

It's hard to read any technology industry news these days without seeing an announcement of a security breach.

Distressingly, the best-intentioned companies all too often find themselves locked into damage-and-spin control, as they seek to help their customers or clients avoid the consequences of identity theft while trying to keep their brands and reputations intact. If you're pondering a potential investment in a systematic and well-executed security process, consider the following cautionary tales carefully.

The real costs of breaches

According to a report by Cybersecurity Ventures and the Herjavec Group, cybercrime costs will grow to $6 trillion by 2021.[1] Many security experts believe the number of breaches is significantly under-reported. It's possible that as many as one of every three businesses experiences one or more security breaches every year.

Increasing frequency of zero-day threats

A zero-day threat is the most dangerous kind of threat that security professionals recognize. When such a threat is discovered it is already doing actual damage, making it imperative to erect some kind of defense immediately. Because dealing with threats takes time—hours or days are common, sometimes longer—this means a zero-day threat always carries a tangible risk of loss or exposure. Most threats exploit previously undiscovered flaws in browsers or website plugins and can affect a large percentage of Internet users.

Increasing costs of security breaches

The Ponemon Institute 2016 Cost of Data Breach study sheds some depressing light on the financial impact of data breaches. The average total cost of a data breach comes to $7.01 million, which represents a 23% increase overall since 2013. Assessed on a per-record basis, the average cost incurred for each stolen or lost record containing sensitive or confidential data increased to $221 per item, of which $145 represents indirect costs (abnormal turnover and customer churn) and $76 direct costs (expenditures to resolve the data breach itself).[2] The takeaway: data breaches are invariably expensive and becoming more so with time.

It's a wild, mad, bad and dangerous world

Though the news is sometimes best understood as a form of entertainment, the excitement that comes from understanding today's threat landscape, and the costs it can bring to organizations, is more scary than fun. Well-run organizations know that best practices, due diligence and even fiduciary and regulatory responsibilities require them to stay ahead of the many bad guys seeking to break in and steal information, assets or valuables.

Now, let's explore how your organization can establish and maintain proper security, and security practices, to minimize your exposure and ensure proper responses to the vast array of threats and risks ready to wreak havoc on your organization.

Bulletproofing is an ongoing practice, not "set it and forget it"

The first, most important thing to understand about information security is that it's an ongoing practice that requires constant vigilance, regular activity and adherence to a set of well-established and well-maintained best practices and processes. The following diagram illustrates a whole methodology that, once established, can be repeated or revisited at regular intervals.

The IT security process

1 Recognize and value information assets

The security process begins with an inventory of what's present and what's worth protecting and monitoring. At the same time, a monetary value needs to be associated with each information asset, so it can be used as a benchmark to guide efforts and expenditures related to securing and protecting that asset. Generally, if the time, effort and expense required to secure and protect an asset exceeds its value, it may not be worth protecting.

IT security process

1. Recognize and value information assets
2. Assess and evaluate risk
3. Establish mitigation and avoidance strategies
4. Consider cyber insurance
5. Understand compliance requirements
6. Establish security policy
7. Measure and monitor security
8. Respond to detected incidents
9. Conduct periodic security audits

2 Assess and evaluate risk

Managing risk is all about recognizing what risks apply to an organization and then deciding which risks to avoid, accept, control or transfer. Some assets are bound to be at more risk than others, often in tandem with their strategic or financial value. For each information asset identified, an assessment of its associated risk must be calculated, so as to prioritize activity, expenditures and attention. The threat landscape plays an important role here, because it provides guidance on what kinds of risks are likely to be encountered, along with associated vulnerabilities and exposures to be handled and managed.

3 Establish mitigation and avoidance strategies

Mitigation involves establishing defensive measures to protect assets, often in the form of multiple layers of security established to reduce risks. When risks cannot be completely mitigated or defended against, they must be avoided. Sometimes, this may mean abandoning an asset, such as a customer directory that reveals contact information in violation of privacy requirements. This may also involve transferring risk to a third party, possibly by purchasing one or more forms of insurance.

4 Consider cyber insurance

Numerous insurance carriers now offer various forms of cyber insurance to cover costs associated with security breaches. This mitigates the risk by offsetting costs involved with recovery and remediation after a cyber-related security breach or similar security incident has occurred. Rooted in errors and omissions insurance (E&O), cyber insurance policies have been available since 2005, with the total value of premiums forecast to hit $7.5 billion by 2020.[3] This insurance covers expenses related to first parties (your organization) and claims from third parties (users, clients or customers affected). Covered costs include those for forensics investigation, business losses, privacy and notification (data breach notification and credit monitoring for clients or customers) and lawsuits and extortion.

5 Understand compliance requirements

In addition to legal and business responsibilities to clients, customers and partners, certain data breaches carry additional legal and regulatory requirements. Some breaches—like those involved with customer account information tied to the PCI framework and/or GLBA legislation or health records tied to HIPAA legislation—even pose the possibility of civil penalties and fines. Specific compliance requirements also include regular security audits and enforced remediation when those audits turn up compliance gaps or omissions.

6 Establish security policy

Ultimately, a security policy defines what assets must be secured and how that is to be accomplished. That's why a security policy covers everything from technical controls over access (password policies, multi-factor authentication, job-role-associated access rights and so forth) to acceptable use policies, administrative policies and auditing, monitoring and reporting requirements.

7 Measure and monitor security

The old saying goes, "If you can't measure it, you can't monitor it." Keeping up with security is how you make sure it's working. This means keeping an eye on assets to ensure their integrity and value remain intact. It also means monitoring systems and networks to make sure no signs of a potential breach or unauthorized access are present. This is the frontline for enforcing a security policy because measurement and monitoring provide empirical evidence for user behavior, access to assets, potential vulnerabilities and possible security exploits. They also provide tangible metrics for use in dashboards and report cards.

8 Respond to detected incidents

If a security breach or exploit is discovered, an organization must have an incident response mechanism in place to deal with the situation. This means dedicating human and technical resources to documenting, containing and remediating the breach. It also means performing an after-the-event analysis to understand its cause(s) and enacting new or enhancing existing policy and controls to prevent any recurrence. An incident response team is usually designated to deal with matters and provided with a response plan to guide their actions, notifications and reporting.

9 Conduct periodic security audits

Either by compliance mandate or by best practice (if not both) organizations must conduct periodic security audits to assess their current security posture, status and compliance where applicable. This effort also involves comparing security policy as documented to security, as enacted and practiced within the organization and as dictated by the current threat landscape. To better implement or match policy, organizations need to alter or enhance their technical controls and guidance. A policy may have to change to reflect evolving circumstances and business needs. Regular auditing provides the incentive to keep things current and ensure they're working properly by cycling back through all the other elements of the security cycle.

What's next?

Now is a great time to secure your inflight data with a dedicated optical network. Wavelength Services from Windstream Enterprise encapsulates data within a transparent optical transport service without additional hardware, enabling you to create your own private network.

The solution's inherent security and reliability protect your business and your customers. Additionally, Windstream Enterprise provides a full range of security services—such as DDoS mitigation and optical Encryption as a Service—that mitigate risks, support compliance requirements and help you take control of your critical data demands.

1 Morgan, Steve. "2017 Cybercrime Report." *Cybersecurity Ventures*, Cybersecurity Ventures sponsored by Herjavec Group, cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf. Accessed 7 Feb. 2018.

2 "2016 Cost of Data Breach Study." *Security Intelligence*, Ponemon Institute, June 2016, securityintelligence.com/media/2016-cost-data-breach-study/. Accessed 7 Feb. 2018.

3 "Insurance 2020 & beyond: Reaping the dividends of cyber resilience." *PwC*, www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf. Accessed 7 Feb. 2018.

About Windstream Enterprise

Windstream Enterprise collaborates with businesses across the U.S. to drive digital transformation by delivering solutions that solve today's most complex networking and communication challenges.

To learn more about network security, visit windstreamenterprise.com

WINDSTREAM
ENTERPRISE

CONNECT. TRANSFORM. ELEVATE.

2958 I 02.18 ©2018 Windstream Services, LLC. All Rights Reserved.