InteliSecure

Quantifying business risk to optimize data security

C-level guidance for protecting a company's most valuable assets

A different lens

Data security has historically been a technical concern handled by technologists. But with nearly $100 billion spent on security solutions annually and high-profile security events continuing to cause significant financial, customer, and reputation losses, the issue has moved out of the data center and into the executive suite.

CEOs, CFOs, and CIOs increasingly want to know how much is being spent on security, where it is being spent, and the effectiveness of those investments. While technology specialists can typically explain the security solutions in place, answers related to risk and ROI are often unknown and difficult to quantify.

With security costs and risks continuing to rise, now is the time to re-examine and optimize data security through a different lens.

Harvard Business Review: Why executives underinvest in cybersecurity

According to Harvard Business Review, determining the ROI for any cybersecurity investment, from staff training to AI-enabled authentication managers, can best be described as an enigma shrouded in mystery. The digital threat landscape changes constantly, and it's very difficult to know the probability of any given attack succeeding—or how big the potential losses might be. Even the known costs, such as penalties for data breaches in highly regulated industries like health care, are a small piece of the ROI calculation. In the absence of good data, decision makers must use something less than perfect to weigh the options: their judgment.

But insights from behavioral economics and psychology show that human judgment is often biased in predictably problematic ways. In the case of cybersecurity, some decision makers use the wrong mental models to help them determine how much investment is necessary and where to invest.

If the focus of cybersecurity programs continues to be on designing better technologies to combat the growing menace of cyberattacks, we'll continue to neglect the most important aspect of security—the person in the middle. By turning the lens of behavioral science onto cybersecurity challenges, executives can identify new ways to approach old problems, and maybe improve their budgets at the same time.

Source

Misguided fears, investments

Most companies are worried about a doomsday scenario: A big cyberattack with malware or ransomware bringing productivity to a halt; a data breach that results in the loss of customer records, passwords, and credit card information; or a hacker getting behind the firewall to wreak havoc or plant clandestine spyware.

Any of these events could create customer, legal, or publicity problems for a company and its executives, and all of them would be costly to resolve. To avoid such situations, most companies are spending mightily on perimeter solutions—like firewalls, endpoint protection products, and intrusion detection systems—that are intended to keep nefarious individuals and viruses out, or at least sound an alarm should they get in.

But these fears and the resulting investments are largely misguided.

Only a small fraction of security events are related to malware, ransomware, and identity theft. Far more prevalent—and more damaging—are the loss or unintended exposure of trade secrets, company plans, and other critical data assets. Many of these leaks come from internal sources. Some are accidental in nature, and most are due to a lack of process development, control, and oversight.

The point is this: The vast majority of security spending is being directed to the areas of least risk.

Company executives wanting to correct this imbalance—to improve their data protection, reduce their security spending, or both—will need to reevaluate their vulnerabilities, strategies, and investments. And they will need to do so through business risk and ROI assessments, not technology evaluations.

The vast majority of security spending is being directed to the areas of least risk.

The biggest gaps

The imbalance of security spending isn't just related to risk vectors, but also to the triad of elements required for effective data protection—people, processes, and technology.

Today, a significant portion of security budgets is being spent on standalone, turnkey technologies—those that don't require data monitoring and investigation, process development and oversight, or risk analysis and optimization. In fact, many companies overbuy and overprovision these solutions, while ignoring other—more risky—areas of vulnerability.

Technology alone can't solve the problem, so it's no surprise that the biggest security gaps are related to a shortage of people and processes. With most security teams being understaffed, company executives have three choices to balance and fortify their human and programmatic resources:

1. Hire new security professionals
2. Retrain and redirect existing workforce
3. Partner with a security services company

With security professionals in high demand, hiring additional specialists or retraining internal staff is both challenging and expensive. And staff turnover is always a concern.

Fortunately, improving data protection doesn't always require a greater investment or staffing changes. Sometimes it's a matter of spending more wisely and leveraging external expertise and resources. Security services companies can bring a wealth of specialists and methodologies to the table, helping optimize the balance of people, processes, and technology. They can also provide critical, business-focused threat assessments and help redirect security dollars to the areas of greatest risk.

Critical data assets, defined

A critical data asset is any piece of information that could cause irreparable harm to an organization should it be lost, stolen, improperly shared, or improperly exposed. Some types of critical data are well-known and regulated pieces of information, such as Protected Health Information (PHI), Personally Identifiable Information (PII), and Payment Card Industry (PCI) data. Other types of critical data aren't regulated but are very important to a company, such as intellectual property, business research and planning information, financial statements, price lists, and merger and acquisition details.

There are ways to forecast the frequency and financial impact of a data breach or loss.

Prioritizing assets

Before risk and ROI assessments can be performed, companies will need to classify and prioritize their data assets—the resources needing protection.

While every organization has a diversity of data assets, these assets are equally diverse in their value to the company. Email archives, legal records, and financial transactions, for example, likely would not have a significant economic impact to a company if they were lost or corrupted. On the other hand, a company's trade secrets, R&D documentation, internal plans, and customer or employee records that contain financial, medical, or other personally identifiable information would be devastating to lose or expose.

The latter represent "critical data assets," and they often align with areas of highest risk.

What constitutes a critical data asset varies by organization and is generally tied to balance sheets, revenue forecasts, operating budgets, and risk models. Given unlimited resources and manpower, all critical assets could theoretically be protected in a comprehensive and continuous fashion. Most security teams do not have unlimited resources, however, so data assets must be categorized and prioritized.

After a company's most valuable information assets have been identified, an assessment of each asset's vulnerabilities can be performed. A "CIA" assessment is commonly used, evaluating the asset's confidentiality, integrity, and availability.

Confidentiality involves an organization's ability to ensure the asset is not accessed in an unauthorized manner while it is being stored, used, or transmitted. Integrity involves an organization's ability to ensure the asset has not been altered in an unauthorized manner or by unauthorized individuals. And availability involves an organization's ability to ensure an asset is accessible by legitimate individuals and groups.

Calculating financial impact

Security is all about risk mitigation, but few companies have formally characterized their risk profile—or quantified the financial impact of such risks. Even as billions are spent and lost due to security risks and events, most security decisions and investments continue to be made from a purely technological perspective.

Although it takes skill and rigor, all business risk is quantifiable.

In its simplest form, it's a matter of identifying the bad things that can happen to a company and the likelihood of those things happening. Taking a cue from the insurance industry—the undisputed experts of analyses that correlate risk with economic impact—financial risk models can be leveraged to tie a company's security program to its bottom line.

First, all potential data security risks and events must be identified, from minor to catastrophic. Direct and indirect costs can then be calculated to determine the Single Loss Expectancy (SLE) of each risk or event. Direct costs of a data breach might include fines for regulatory violations, hiring a PR firm to repair the company's image, and purchasing technologies or services to prevent a recurrence. Indirect costs might include damage to brand reputation, loss of customers, and reduction in sales.

Next, how often these incidents are likely to occur over the course of a year must be estimated, leading to the Annual Rate of Occurrence (ARO) for each event.

While indirect costs and ARO are much more difficult to quantify than direct costs, there are ways to forecast the frequency and financial impact of a data breach or loss. It often requires the analysis and correlation of multiple data points—internal and external, current and historical—leading to educated guesses and documented assumptions.

The SLE for each event can then be multiplied by its ARO, revealing the Annual Loss Expectancy (ALE) of that particular event. ALE is the quantification of a specific risk, showing the expected economic impact to the business on an annual basis.

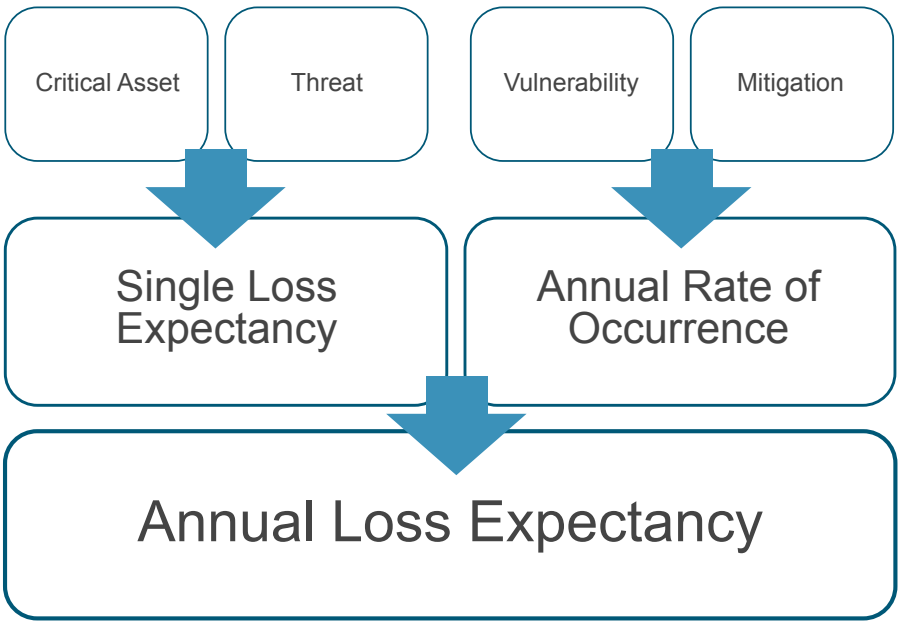
Modeling risk

With a clear understanding of critical data assets and their vulnerabilities as well as the likelihood and financial impact of security-related events, companies can conduct a formal risk modeling exercise. The exercise is designed to model the risk that exists at the present moment, revealing strengths and vulnerabilities that can help optimize spending and data security.

To reiterate, critical assets represent the data in an organization that need the highest levels of protection. Threats are the identified scenarios that may cause harm to these assets. When evaluating the critical asset in conjunction with the bad things that could happen to that asset, an organization can project the financial impact of each event, or the SLE.

On the other side of the model, the vulnerability of each asset's confidentiality, integrity, and availability is compared to mitigation techniques currently in place. The result is a decimal-based probability that represents the number of times the vulnerability is expected to be exploited per year, known as the ARO.

The SLE multiplied by the ARO will yield an ALE, or the estimated annual financial impact of a specific threat against a specific critical data asset.



Three categories of data

After data assets are identified, they must be prioritized.

1. Shared – available to anyone
2. Sensitive – limited sharing with specific individuals or groups
3. Critical – secret/internal, never shared

Four categories of risk

After risks are identified, decisions must be made about how they will be handled.

1. Accepted – maintaining the status quo
2. Mitigated – employed for the majority of identified risks
3. Avoided – generally impractical unless data assets are eliminated
4. Transferred – insurance policies that cover direct costs only, with severe limitations

The modeling exercise, while relatively simple, brings a new perspective to data security risks and business exposure. And it helps bridge the sizeable gaps between technology specialists and business leaders.

It not only allows existing security vulnerabilities and their anticipated financial impact to be quantified, but the benefits that can be attained if those vulnerabilities are addressed can also be calculated. In doing so, it allows organizations to optimize their security investments—focusing on the greatest areas of risk—and get the most benefit for the least cost.

Many enterprises have an overabundance of intrusion detection systems, but they've handed out too many keys and their valuables are on the front table.

McKinsey: Top management must lead critical data protection efforts

According to McKinsey & Company, top executives must lead an enterprise-wide effort to find and protect critically important data, software, and systems as part of an integrated strategy to achieve digital resilience.

In determining the priority assets to protect, organizations will confront external and internal challenges. Businesses, IT groups, and risk functions often have conflicting agendas and unclear working relationships. As a result, many organizations attempt to apply the same cyber-risk controls everywhere and equally, often wasting time and money but in some places not spending enough. Others apply sectional protections that leave some vital information assets vulnerable while focusing too closely on less critical ones. Cybersecurity budgets, meanwhile, compete for limited funds with technology investments intended to make the organization more competitive. The new tech investments, furthermore, can bring additional vulnerabilities.

The work to prioritize assets and risks, evaluate controls, and develop remediation plans can be a tedious, labor-intensive affair. Specialists must review thousands of risks and controls, and then make ratings based on individual judgment. Some organizations mistakenly approach this work as a compliance exercise rather than a crucial business process. Without prioritization, however, the organization will struggle to deploy resources effectively to reduce information-security risk. Dangers, meanwhile, will mount, and boards of directors will be unable to evaluate the security of the enterprise or whether the additional investment is paying off.

Source

Achieving balance

At the end of the day, data security is all about balance—of spending and risk.

Once risks are understood and quantified from business and financial perspectives, organizations can begin to evaluate the effectiveness and ROI of their security program. How much is the company spending on data security? Are those investments effective? Do they protect the organization's most valuable data assets and mitigate its biggest risks? What would happen if those investments are increased, reduced, or reallocated?

Risk modeling reveals the answers, providing a business-level analysis of data security that is increasingly required by CEOs, CFOs, and CIOs. And it facilitates the rebalancing and optimization of security spending and risk mitigation.

Because budgets and resources are always limited, there is no way to fully protect everything at all times. Companies must carefully select where and how they spend their security dollars, focusing on the assets of most value and the areas of greatest risk.

Home security offers a fitting analogy.

Most individuals want to secure their home and protect the belongings inside. It would be financially impractical to turn the entire house into a massive safe or vault, however, and it would also be risky to leave valuable possessions on a table within full view of a front window. The best protection would arguably be a combination of locked doors and windows, a home security system that offers intrusion detection, and a hidden safe that contains the owner's most valuable possessions.

Today, many enterprises have an overabundance of intrusion detection systems, but they've handed out too many keys and their valuables are on the front table.

Data security is all about balance – of spending and risk.

About InteliSecure managed security services

Perimeter-only security programs continue to be ineffective against today's persistent threats.

That's why InteliSecure, unlike traditional managed security service providers (MSSPs), is laser focused on protecting your most critical data assets—based on revenue, income, reputation, and core operational impact—at the perimeter and everywhere else.

Combining people, process, and technology, InteliSecure's proven Critical Data Protection Program™ methodology safeguards your most sensitive assets from malicious and accidental breaches, whether from external or internal sources. The result is a more targeted and effective security posture.

InteliSecure

To learn more, visit www.intelisecure.com

InteliSecure industry firsts

- One of the first 10 organizations recognized as an ISO 27001 Associate Consultant by the BSI Group (2006)
- First MSSP to offer managed DLP services (2008)
- First MSSP to combine machine data with heuristics-based analytics for content and context based approach (2008)
- First MSSP with a focus on critical asset protection programs across all services—data and threat protection (2013)