Ransomware: Executive Summary

(for Non-Technical Executives)

C-Suite Brief: Business Statistics & Simple, Inexpensive Ways to Test Your Exposure to Ransomware

What Business Leaders Need to Know

While you're making daily efforts to grow your organization and service your customers, cybercriminals are making parallel efforts to **cripple your business through ransomware attacks.** This risk will only continue to grow as new ransomware groups appear annually and threat actors actively leverage new tactics.

Seven critical data points that every business leader needs to be aware of:

1. 80% of companies have experienced one or more ransomware attacks, and of those:[1]
   - 53% of respondents reported paying the ransom.
   - Ransom payments averaged over $1 million.
   - 64% of respondents did not have cyber insurance policies that covered ransomware.

2. 42% of organizations affected by a successful ransomware attack experienced some level of business disruption. The average amount of business downtime was six days, but for 37% of those incidents, this downtime lasted for over one week.[2]

3. 25% of all breaches in 2022 involved ransomware.[3]

4. $9.44 million was the average cost of these 2022 breaches in the U.S[4]

5. **53% of IT experts admit they don't know how well the cybersecurity tools they've deployed are working.**[5]

6. Cyber insurance premiums increased by an average of 28% in the first quarter of 2022 compared with the fourth quarter of 2021.[6]

7. For public companies, in 2022, the Securities and Exchange Commission proposed expanded rules to further enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and cybersecurity incident reporting. Proposed rules include:
   - Disclosing material cybersecurity incidents on Form 8-K within four business days.
   - Providing disclosures in Form 10-K about (1) cybersecurity monitoring and risk management policies and procedures, (2) management's role in implementing those policies and procedures, and (3) cybersecurity governance, including oversight by the board of directors.

There Are Solutions

At the risk of sounding like Captain Obvious from the Hotels.com commercials, cyber risk is no longer simply a technology issue — **it's a business issue.**

Failures in information security result in significant, costly consequences for your organization. Subsequently, C-level executives and board members must become increasingly educated in this domain.

Current facts and data do not favor organizations in their efforts against malicious actors.

The good news, though, is that there are **simple, cost-effective solutions** to:

- Measure the efficacy of your cybersecurity controls and investments.
- Close security gaps that currently and unknowingly exist within your organization.

Importantly, and detailed in this brief, a ransomware assessment does not require your organization to purchase additional security tools and **can be accomplished in a matter of days.**

Test Your Security Controls

The concept of testing your software has been around for decades. Organizations' software development teams *would never think of deploying software without a thorough QA process intent on detecting, and remediating, bugs of a certain severity level.*

When it comes to cybersecurity tools and controls, however, most organizations don't take this same testing approach.

This is a real head scratcher (which brings to mind the cartoon character Scooby Doo: "Ruh Roh!")

As an executive, your thought might be, "Well, we don't build those tools — we buy them. That testing is clearly done by the software vendor."

Although this thinking isn't necessarily incorrect, it completely misses the fact that your organization's system administrators and security tool engineers *are the ones responsible for the deployment, **configuration**, and maintenance of these tools.*

1 | For instance, Cloud Service Providers (CSPs, or hosting platforms such as Amazon AWS, Microsoft Azure, and Google's GCP) *provide tools* to help manage cloud configuration. But it is the *responsibility of your technology employees to configure these tools.* **Misconfiguration of cloud resources remains the most prevalent cloud vulnerability and can be exploited to access cloud data and services.**[7]

2 | When it comes to your network security — your firewalls — Gartner estimates that 99% of firewall breaches are caused by firewall misconfigurations, not firewall flaws.[8]

Many of these misconfigurations are simple in nature — human error. To err is human, and your employees and/or contractors — unknowingly, unintentionally — are many times the No. 1 cause of the holes in your cyber defense.

These same holes are the entry points through which malicious actors gain access to your network. That's why it's crucial to discover them through testing before threat actors do.

You might already be performing annual penetration (pen) testing, but pen testing has significant limitations, including:

- The timing and scope of testing is extremely limited.
- As a result, you can't come even close to covering all your vulnerabilities and threats.

How to Best Test and Validate Your Security Controls

There are many mature, mainstream technologies that **test your security tools and controls.**

These tools are both easy to deploy and inexpensive relative to the (a) financial losses and (b) lost business continuity attached to a breach and/or ransomware attack.

These solutions go by several terms, the most common are which:

- Security Validation
- Continuous Security Validation (CSV)
- Breach & Attack Simulation (BAS)

Importantly, these tools can be deployed into your environment in a matter of hours (not days, weeks, or months).

In short (and in non-technical language for this executive audience), here is how these software solutions use automated testing to **provide you with increased assurance that your security controls are working as intended:**

1 | Security validation tools have created libraries of thousands of known methods of how attackers breach your network.

2 | These tools deploy a sensor to different components of your network, such as an endpoint like a laptop, your email server that processes all inbound and outbound email traffic, or your firewalls through which all inbound and outbound traffic traverses your network.

3 | Security validation or BAS solutions then – in a safe manner, as these are not *actual* attacks – **simulate attacks** against these different components of your "security stack" (the different tools in your security portfolio).

4 | The sensors that were put in place detect these simulated attacks in those instances where your security tools failed to properly detect them.

5 | Reports are generated indicating which controls failed and why.

6 | This allows your InfoSec or technology teams to remediate failures before an *adversary uses them to your disadvantage*.

SP6 has published a more in-depth Guide to Breach & Attack Simulation (BAS). This publication is a broader overview intended for both non-technical and technical audiences.

SP6 has also published a brief on ransomware for technical audiences. This brief dives into the types of ransomware that organizations face and the technical nuances of how BAS tools work.

Test Against Ransomware with SP6's Ransomware Assessment

SP6

SP6 has designed a **simple, cost-effective** CSV/BAS service offering focused specifically on ransomware with the following attributes:

- It is conducted in **one week or less.**
- **It does not require your organization to make an investment in, nor manage, yet another technology tool.** (SP6 leverages the Security Validation / Breach & Attack Simulation software, highlighted above, as the central mode for this testing).
- It offers **different methods, or levels, of testing.** Just as malicious actors attack your network in various ways, SP6's Ransomware Assessment gives you various options as to what to test. Based on the probability of attack vector, we can provide advisement on the scope of testing.
- It provides your InfoSec team with a report that illustrates **exactly where your security controls failed** and, subsequently, what controls your team needs to remediate.
- It is a **minimal investment** when compared to well-documented benchmarks of the probability and cost of a breach.

Don't Forget

Ransomware in and of itself is simply a **model of monetizing** a breach of your organization's security controls. There are several key **paths** that threat actors traverse to invade your network and enable their unauthorized access. Using these pathways, ransomware is malware (malicious software) that uses encryption to hold your information at ransom.

Common routes ransomware uses to invade your network include:

- Unauthorized access of credentials
- Exploiting vulnerabilities
- Exploiting misconfigurations (as mentioned above)
- Phishing
- Botnets

Your security team has a host of security controls – both policies and tools – that address many of these attack methods.

Are you testing them for efficacy?

Conclusion

In summary:

- Cybersecurity risk is a business problem, not a technology problem. This exposure carries outsized, expensive risks. C-level executives need to be both knowledgeable of and part of the solution.
- Empirical data from independent, third-party research firms have quantified the cost of this exposure, as well as the probability of your organization being affected. Some of this data is shared above.
- Despite testing software prior to deployment and ongoing releases, most InfoSec programs don't test their security controls. Simply put, this is ludicrous, given the:
  - high probability of an actual breach (with or without ransomware attached);
  - level of financial loss tied to a breach;
  - amount of time, money, and resources your organization invests in cybersecurity.
- There are methods to test your cybersecurity controls.
- The time and cost attached to these testing methods are minimal relative to the financial exposure of a breach.

About SP6

SP6 is a niche technology firm specializing in cybersecurity, cyber compliance (with a heavy emphasis on CMMC), and systems availability. Our organization is committed to ensuring that clients and their systems are secure, compliant, and highly performant.

Request a Conversation

For more information, visit **www.SP6.io**

or contact us at **Service@SP6.io**.

Citations

[1] Ponemon Institute, sponsored by Converge Security. Ponemon (www.ponemon.org) is an independent research firm, highly recognized in the technology space, focused on empirical studies on critical issues affecting the security of information assets and the IT infrastructure. (2021). This report included a sampling frame composed of 15,577 individuals in the United States responsible for containing ransomware infections within their organization were selected for parrcipaaon in this survey. As shown in Table 2, 716 respondents completed the survey. Screening removed 57 respondent surveys. The final sample was 659 respondent surveys (or a 3.7 percent response rate). 56% of participants were supervisory levels of greater (Supervisor, Manager, Director, VP or C-level).

[2] Hanover Research, "State of Ransomware Readiness Report", which surveyed 742 cybersecurity professionals globally (September 2021). 19% of respondents worked in organizations with 5,000 employees or more; 49% with 1,000 to 4,999 employees, 32% with under 1,000 employees.

[3] Verizon Data Breach Investigations Report (2022)

[4] Cost of a Data Breach Report 2022, conducted by independent research firm Ponemon Institute and sponsored by IBM. The 2022 report was conducted via over 3,600 interviews with individuals from 550 organizations that were impacted by the data breaches, across 17 different industries. These organizations were impacted by data breaches that occurred between March 2021 and March 2022. Cost figures include:

- *Detection and escalation*
  – Forensic and investigative activities; Assessment and audit services; Crisis management; Communications to executives and boards
- *Notification*
  – Activities that enable the company to notify data subjects, data protection regulators and other third parties, including the following: Emails, letters, outbound calls or general notice to data subjects; Determination of regulatory requirements; Communication with regulators; Engagement of outside experts
- *Post breach response*
  – Activities to help victims of a breach communicate with the company and redress activities to victims and regulators, including the following: Help desk and inbound communications; Credit monitoring and identity protection services; Issuing new accounts or credit cards; Legal expenditures; Product discounts; Regulatory fines
- *Lost business*
  – Activities that attempt to minimize the loss of customers, business disruption and revenue losses, including the following: Business disruption and revenue losses from system downtime; Cost of losing customers and acquiring new customers; Reputation losses and diminished goodwill.

[5] Ponemon Institute (www.ponemon.org) surveyed 577 IT and IT security practitioners in the United States who are knowledgeable about their organization's IT security strategy and tactics. More than half of respondents (58%) were at or above the supervisory levels. Ponemon is an independent research and education firm in the area of information and privacy management practices.

[6] Council of Insurance Agents & Brokers (CIAB), an association for commercial insurance and employee benefits intermediaries.

[7] National Security Agency (NSA), "Mitigating Cloud Vulnerabilities" report, https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF

[8] Gartner, www.gartner.com (Subscription required)