5ironCYBER

FOCUS

Prioritizing What Matters Most in Life and CyberSecurity

Jeremy Hopwood
CEO, 5ironCyber

We want to challenge your thinking and offer a different perspective.

At your firm:
Is Cybersecurity a necessary evil
(a grudge purchase) . . .

(or) an ongoing investment?

HINT: if it is an investment, *you will put more than $ into it.*

5ironCYBER

https://www.micromindercs.com/blog/cybersecurity-grudge-purchase-or-investment

Table Stakes . . .

5ironCYBER

Focus

25

5ironCYBER

5

FOCUS

Warren Buffet’s concept was about *Personal Success*.
Where can you put his 25/5 plan into place personally?

- Professional Growth
- Health & Wellness
- Financial Stability & Wealth Building
- Relationships
- Personal Development

We can use the same concept to help us succeed in our battle against cyber threats.

Start with the END in mind....

If we know that EVERY company will be compromised—it is just a matter of *WHEN* not IF . . .

. . . Then we should look at the problem very differently.

Average cost of a breach in 2023 was $4.8M

5ironCYBER

2024 IBM Cost of a Data Breach Report, page 5

FOCUSED PRIORITIES

5ironCYBER

SURVIVAL

- **Ensure Business Continuity and "Survival" of the event.**
- **Backups**
- **Insurance**
- **Have Plans Established**—Disaster Recover, Business Continuity, and a Cybersecurity Incident Response (IR) plan.

CYBER FACT

60 percent go out of business within six months of falling victim to a data breach or cyber attack.

https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/

END USER : Training and Accountability

Invest in training . . . It will pay dividends.

- Not just a nod to training, minimal phishing training, or once a year. Instead, develop a cohesive plan.
- Consider real penalties (such as remove hyperlinks from their email after clicks, take away internet access, or put them in a browser isolation group)
- Bring in experts – help them understand the real impact.

5ironCYBER

CYBER FACT

68%

of breaches involved a human element

28%

of breaches involved Human Errors

5ironCYBER

2024 Verizon Data Breach Investigations Report: page 7/17 of executive summary):

VISIBILITY

Make sure your firm has VISIBILITY to the things that matter:

- **Reporting – Board level, and C-level**
- **Ensure you have a SIEM**
  (Security Information and Event Management)
  - The SIEM will collect data and correlate across all security apparatus, giving you visibility to the critical events happening on your network.
- **Regular Gap Analysis**
  - Not by asking your team, but by bringing in experts

ADD BOARD/AVISORY EXPERTISE

- You should not do work you are not qualified to do.
  (Don’t just start drilling the tooth yourself.)
- Always good to have another perspective and counsel
- Make sure that you have proper reporting and metrics around your Cybersecurity program and that you have the right KPIs and metrics measuring success.
- KNOW the Cybersecurity Maturity model and your posture/score.
- Compare to your industry peers
- Seek counsel from trusted C-level peers and ask about what they are doing to “MOVE THE NEEDLE”.

REAL-WORLD SCENARIOS & TESTING

- Build and maintain a strong cyber defense capability with proactive threat hunting powered by strong intelligence.
- Engage with red teams to test defenses and identify gaps and measure the time it takes security teams to identify and respond to compromises.
- Test your ability to detect the latest and most relevant malware, exploits, and initial infection vectors, and conduct regular testing for all employees such as phishing awareness.
- Use tabletop and other exercises to establish protocols, and ensure all employees involved in an incident response are ready to react—especially when it comes to being notified of a compromise externally.
- Practice sound security fundamentals such as vulnerability and exposure management, least privilege, network segmentation, and hardening.

PRIORITIZE ADEQUATE STAFFING

Augmented Support and Expertise . . .

. . . and ENSURE AFTER HOURS COVERAGE.

COVERAGE = the ability to detect, identify, triage and mitigate a real-world threat after business hours* WITH THE SAME or BETTER *level of expertise as you have during first shift.

"Two is one and one is none"

If you PLAN for a single solution, you are planning for failure. Instead, plan for contingency and backup.

5ironCYBER

CYBER FACT

Most cyber-attacks (including ransomware) happen at night.

Most commonly from 1-5am . . .

. . . And on US holidays.

5ironCYBER

Malwarebytes 2024 State of Ransomware Report

CYBER FACT

26.2%

Increase in Cybersecurity skills shortage, over the prior year.

(Note, there are over 500,000 cybersecurity unfilled job postings in the US alone) We are going to need to augment with trusted partners.

5ironCYBER

IBM Cost of a Data Breach Report 2024

WARNING

Avoid “Checkmark” Partners

Many enterprise providers simply want to ALERT you to the threat. Many do not even offer services to mitigate the threat.

BUILD / ENHANCE 3RD PARTY RISK PROGRAM

- **Target, Marriott/Starwood, Equifax, SolarWinds**—and multiple other companies since.
- Most adversaries will not attack large Enterprise companies direct, as those groups spend $MM on Cybersecurity.
    - The adversaries attack softer targets—**supply chain**.
- **Group your 3rd party vendors into groups:**
    - Critical, High, and Low.
- We have had multiple clients that had to notify their clients of an incident, that was caused by a 3rd party provider.

CYBER FACT

15%

of breaches involved 3rd parties

5ironCYBER

2024Verizon Data Breach Investigations Report: page 7/17 of executive summary):

WHAT ARE YOUR

5?

(Personally & Professionally)

5i 5ironCYBER

Questions

5ironCYBER

FOCUS

Prioritizing What Matters Most in Life and CyberSecurity

Jeremy Hopwood
CEO, 5ironCyber