RR

IT AND CYBERSECURITY PROS: DEVELOP YOUR PERSONAL RESILIENCE

December 2024

Derek E. Brink, CISSP
Vice President and Research Fellow, Cybersecurity and IT GRC

ABERDEEN
STRATEGY & RESEARCH
ILLUMINATE. INSPIRE. IGNITE.

In collaboration with: zscaler™

Executive Summary

Today's IT and Cybersecurity professionals are sharply focused on keeping their *organizations* flexible, adaptable, responsive, and resilient. But *personal resilience* for tech pros — i.e., complementing your "hard skills" in technologies by also investing in the "soft skills" of people and processes that make these goals happen — mustn't be overlooked. Our goal is organizational resilience, but supporting and strengthening tech pros in these areas is key to how we get there.

Great Progress in Organizational Resilience

Enabling organizational resilience is challenging enough, given today's technology trends that include:

- A **diverse user base** (employees, partners, suppliers, and customers), which for most organizations includes a combination of **remote/hybrid**
- **Fast, secure, and compliant access** to **cloud-based applications and data** from **anywhere, on any device**
- Expectations for **great digital experiences**, with **business continuity** as a top priority

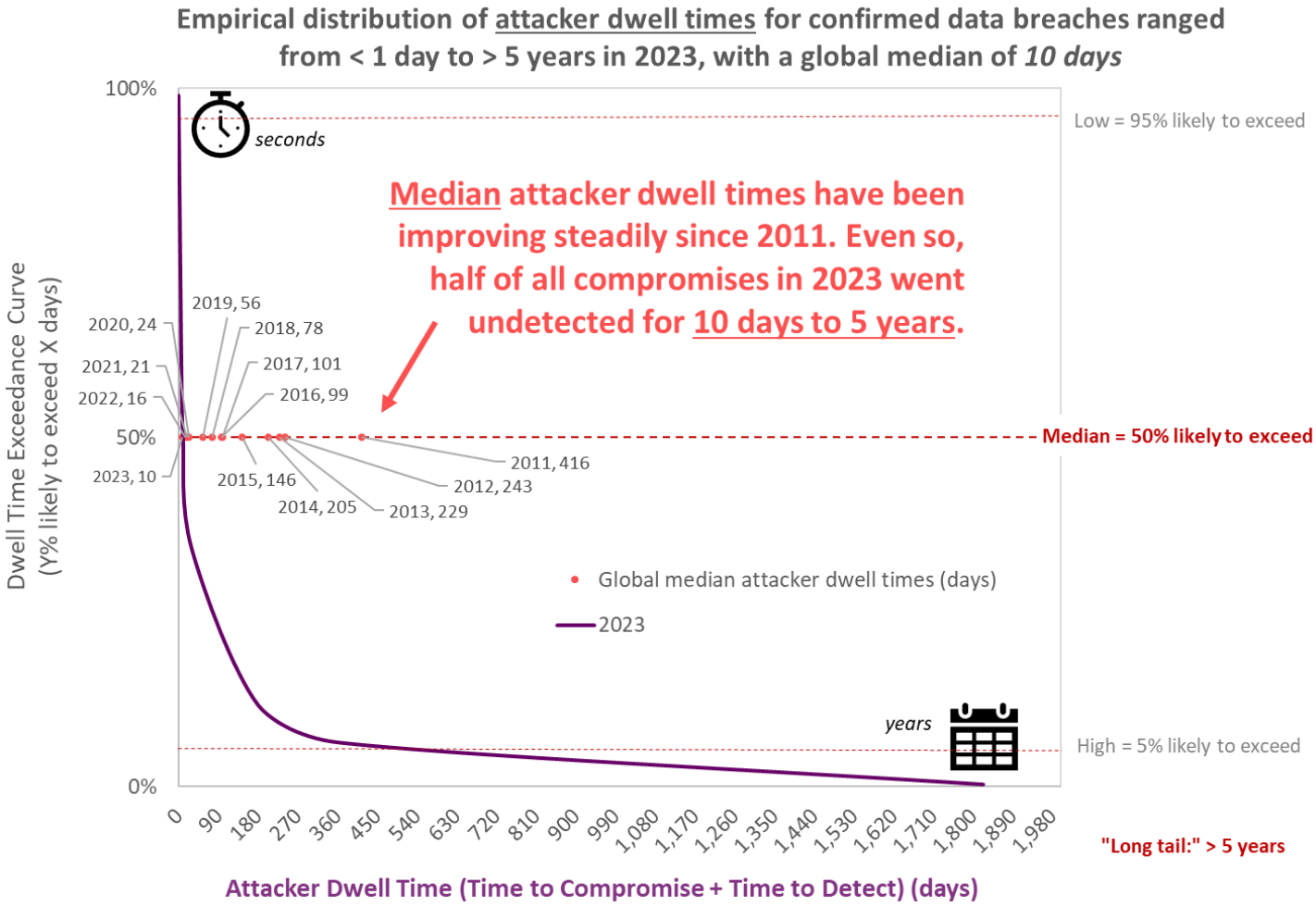
Over the last dozen years, IT and Cybersecurity pros have been focused on detecting and responding more quickly to security incidents and have made significant improvements. The chart in Figure 1 is based on empirical data for *attacker dwell times* — the amount of time attackers remain undetected on compromised systems — published annually by the cybersecurity investigative firm Mandiant (now part of Google Cloud).

In particular, note that:

- The empirical distribution of attacker dwell times for confirmed data breaches ranged from *less than 1 day to more than 5 years* in 2023, with a *global median of 10 days*.
- Median attacker dwell times have been improving steadily since 2011 (a shocking 416 days); even so, half of all compromises in 2023 still went undetected for *10 days to 5 years*.

See *Are You Enabling a Resilient Workplace? A Conversation with Aberdeen Strategy & Research*

Figure 1: IT and Cybersecurity Pros Have Made Significant Improvements in Organizational Resilience



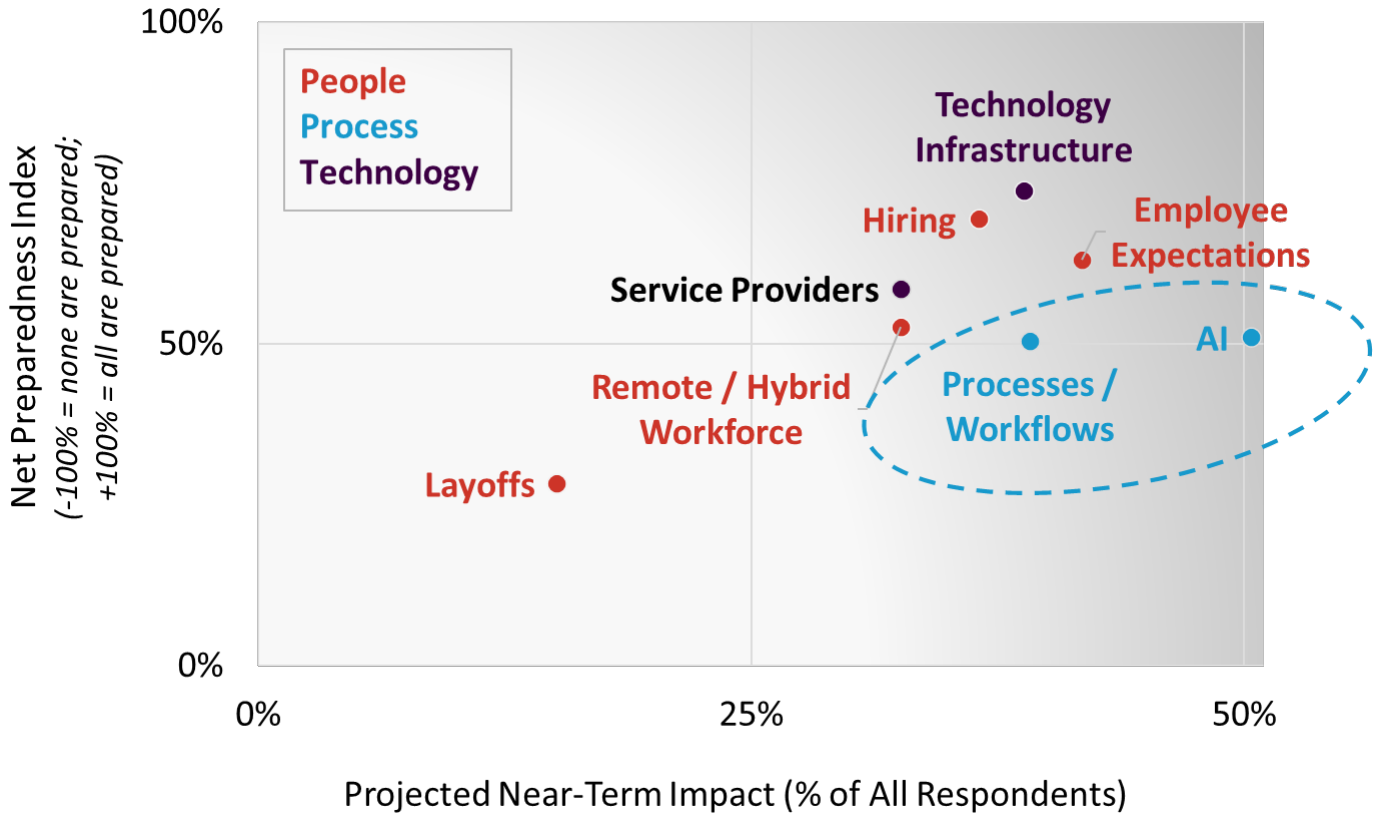
Source: Empirical data adapted from Mandiant *M-Trends* 2011-2013; Aberdeen, December 2024

What About Personal Resilience?

Aberdeen's 2024 *Future of Workplace* study asked respondents about the **projected near-term impact** of several environmental changes, along with **how prepared** they and their organizations are to manage these impacts. Based on these research findings, we see in Figure 2 that personal resilience applies to all three traditional areas of *people*, *process*, and *technology* — and that organizations are **generally confident** in their preparedness for managing the impact of virtually all environmental changes they see coming in the next 12-18 months.

Relatively speaking, they feel the least prepared for high-impact initiatives involving business processes and workflows, which highlights the need to increase personal resilience in the organization's initiatives involving **automation** and **AI**.

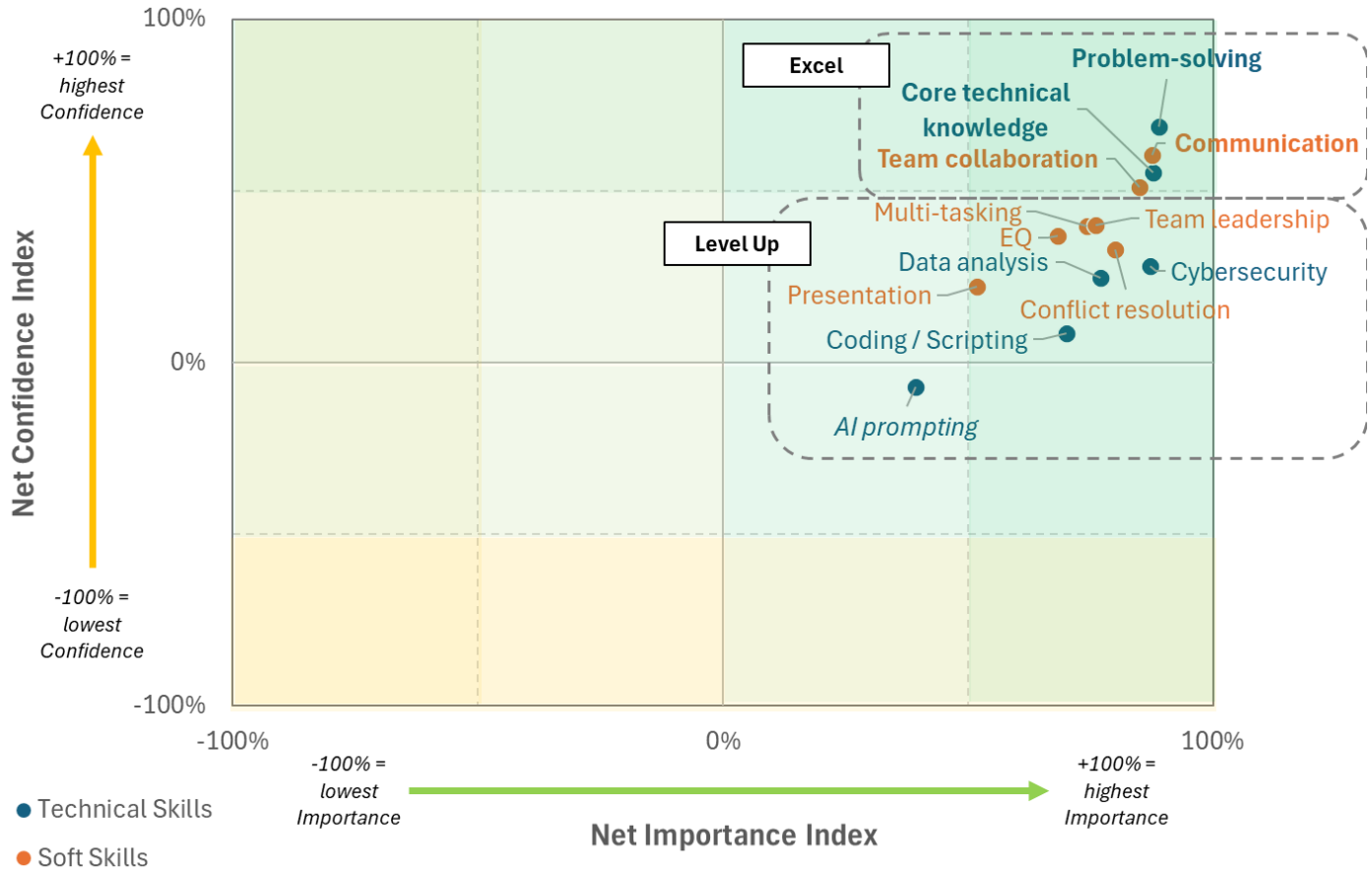
Figure 2: Tech Pros Highlight the Need to Increase Their Personal Resilience in High-Impact Initiatives Involving Automation and AI



Source: Aberdeen, December 2024

Taking this a bit further, the Spiceworks Ziff Davis *State of IT 2025* report asked technical professionals about a representative set of technical skills and "soft skills," in two dimensions: how *important* the skills are, and how *confident* they are in each of these areas. See Figure 3.

Figure 3: Where Tech Pro Confidence in Skills Meets Importance — Four Skills Where They Excel, and Nine Opportunities Where They Might Level Up



Source: Adapted from Spiceworks Ziff Davis *State of IT 2025* report; Aberdeen, December 2024

Based on these findings, here are four areas where Tech pros currently excel:

- **Hard skills:** *core technical knowledge*, *problem-solving*
- **Soft skills:** *communication*, *team collaboration*

Similarly, here are nine opportunities Tech pros might have to level up:

- **Hard skills:** *cybersecurity*, *data analysis*, *coding/scripting*, *AI prompting*
- **Soft skills:** *multi-tasking*, *team leadership*, *presentation (verbal communication)*, *conflict resolution*, *emotional intelligence (EQ)*

In general, descriptors for Tech pros who have developed their personal resilience might include:

- The ability to handle incidents with agility and composure; grace under pressure
- The ability to stay calm and make good decisions when everything hits the proverbial fan
- The mental and operational "muscle memory" to respond and recover effectively from incidents
- Strong communication, presentation, collaboration, and problem-solving skills
- A mindset of continuous learning

Personal Resilience, as Seen in Selected Real-World Examples

A few real-world examples of cybersecurity incidents that illustrate key dimensions of personal resilience are captured in Table 1.

Table 1: Personal Resilience, Exemplified in Real-World Incidents

Incidents Requiring Personal Resilience (illustrative)	Personal Resilience Traits
Cyberattack on the UK National Health Service. The 2017 *WannaCry* attack on NHS resulted in significant operational disruptions, resulting in high-stress conditions for IT staff and employees to maintain healthcare services and minimize harm.	• Crisis Management • Problem-Solving • Collaboration
NotPetya attack on Maersk. When shipping giant Maersk was hit by the *NotPetya* ransomware in 2017, its global operations were brought to a halt. Maersk's IT teams responded by rebuilding their entire IT infrastructure in just 10 days.	• Crisis Management • Adaptability • Innovation
Ransomware attack on the Düsseldorf University Hospital. This 2020 incident led to the tragic death of a patient due to system failure, highlighting the potentially immediate consequences of cybersecurity breaches on public services. IT and healthcare professionals responded swiftly under extreme pressure to restore systems, manage communications, and adapt protocols.	• Crisis Communication • Problem-Solving • Continuous Learning
Evolving Technologies and Regulatory Responses. Regulatory focus on governance and ethical standards for Artificial Intelligence (AI) in EU countries highlights the dynamic nature of technology, regulation, and their impact on cybersecurity.	• Continuous Learning • Cross-Cultural Communication and Collaboration

Cyber Threats to Critical Infrastructure. Several recent incidents targeting critical infrastructure in multiple EU countries highlight the potential complexities of *regulatory* and *cultural* aspects of personal resilience.	• Continuous Learning • Cross-Cultural Communication and Collaboration • Context-Specific Adaptability

Source: Aberdeen, December 2024

Tying it All Together: How Personal Resilience for Tech Pros Helps to Drive Strategic Outcomes for the Business

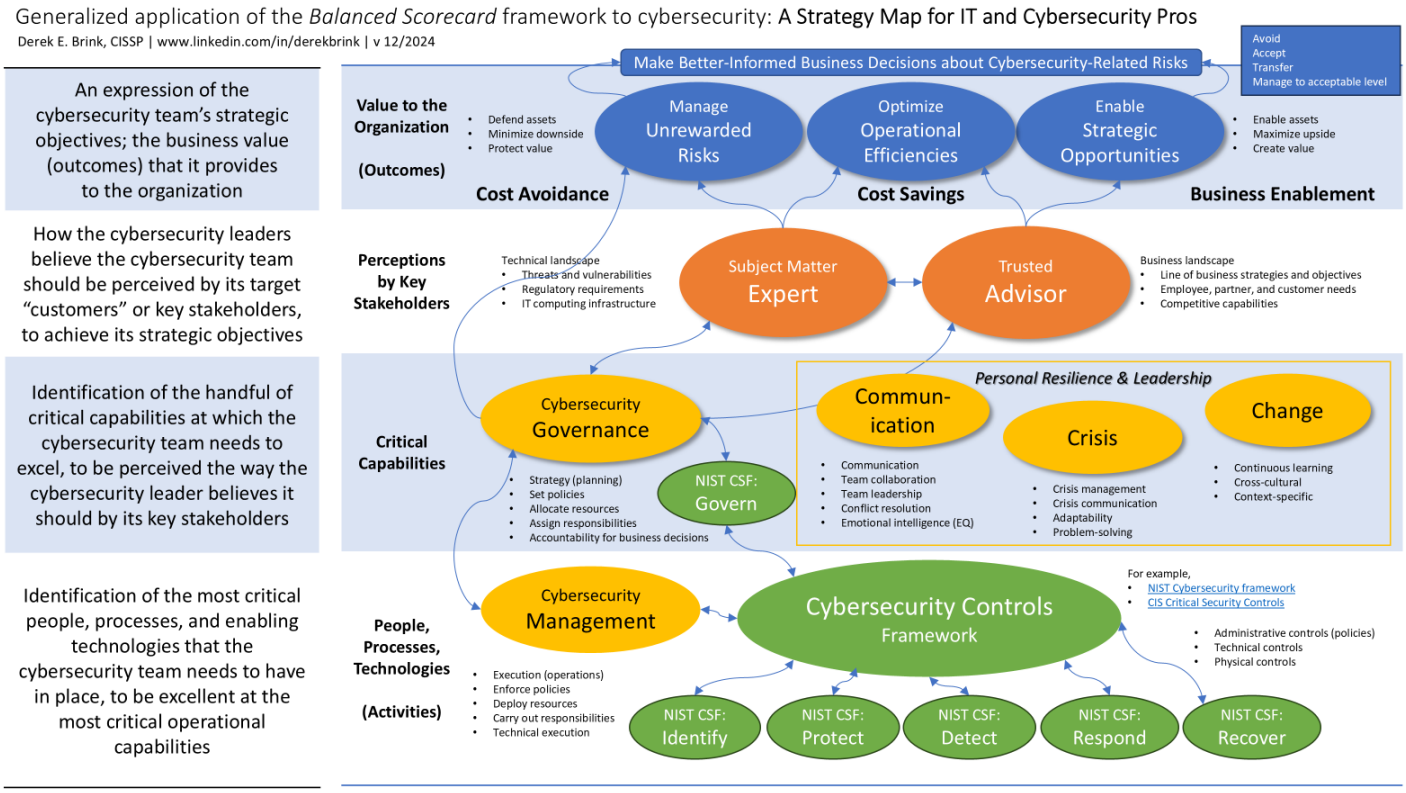
Aberdeen has written about the importance of **connecting technical activities and key capabilities with business outcomes** for many years. One of the most useful visualizations of this is *"A Strategy Map for IT and Cybersecurity Pros"* (see Figure 4), which is Aberdeen's generalized application of the popular *Balanced Scorecard framework* to the topic of cybersecurity.

Since 1992, the *Balanced Scorecard framework* has helped organizations describe, communicate, and execute their strategies by focusing on the cause-and-effect linkages from technical **activities** (people, processes, and technologies) to strategic business **outcomes**.

The Balanced Scorecard is typically defined from the top down — i.e., starting with the strategic business outcomes in mind — but it is always executed from the bottom up. Aberdeen's take on the connections between the four levels of the Balanced Scorecard framework — that is, from *activities*, to *critical capabilities*, to *perceptions by key stakeholders*, to *strategic outcomes* — as applied to cybersecurity is shown in Figure 4 below.

- The characteristics of "personal resilience" discussed previously can be seen in yellow as Critical Capabilities (row 3).
- These are the "soft skills" that help today's technical professionals to complement their traditional "hard skills" in technologies (row 4).
- In turn, these personal resilience characteristics help tech pros to be perceived by key stakeholders as both Subject-Matter Experts and Trusted Advisors (row 2).
- Ultimately, these are the cause-and-effect linkages that deliver the strategic business outcomes related to organizational resilience (row 1).

Figure 4: How Personal Resilience is Key to Driving Strategic Business Outcomes



Source: Aberdeen, December 2024

Summary and Key Takeaways

- IT and Cybersecurity professionals have made great progress in **organizational resilience** over the past several years.
- For today's tech pros, Aberdeen's research highlights the need to increase their **personal resilience** as well.
- Key characteristics of personal resilience can easily be seen in **real-world examples** of cybersecurity incidents.
- Investing in the "soft skills" of personal resilience will help today's technical professionals to complement their traditional "hard skills" in technologies; together, they help to deliver the **strategic business outcomes** related to organizational resilience.

Related Research

- *Are You Enabling a Resilient Workplace? A Conversation with Aberdeen Strategy & Research*; November 2024
- *IT and Cybersecurity Pros: What About Your Personal Resilience? A Conversation with Aberdeen Strategy & Research*; December 2024

About Aberdeen Strategy & Research

Aberdeen Strategy & Research (a division of Spiceworks Ziff Davis), with over three decades of experience in independent, credible market research, helps **illuminate** market realities and inform business strategies. Our fact-based, unbiased, and outcome-centric research approach provides insights on technology, customer management, and business operations to **inspire** critical thinking and **ignite** data-driven business actions.