Most Companies Overestimate Their Cybersecurity, but Resilience Is Possible

Strong cybersecurity is about more than technology; it also takes a long-term commitment to develop a range of strategic capabilities.

By Frank Ford and Syed Ali

BAIN & COMPANY

Frank Ford is a partner and Syed Ali is an expert vice president with Bain's Enterprise Technology practice. Frank is based in London, and Syed is based in Houston.

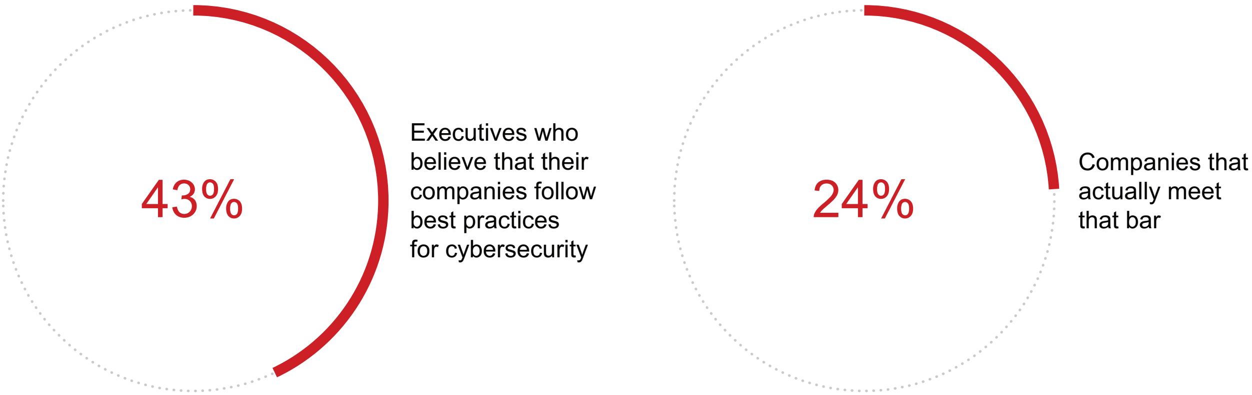
At a Glance

- Companies are spending more than ever to protect against cyberattacks, but this may be creating a false sense of security.
- Investing in great technology is helpful, but it isn't enough. Companies can still leave themselves vulnerable through a wide range of missteps, such as failing to focus their investments on their most important assets or not supporting their people and partners with good training.
- True resilience comes only with sustained dedication to building up a broad range of strategic capabilities and developing cybersecurity maturity.

Few executives need to be told that cybersecurity is a critical issue, one that is central to protecting an organization's assets and reputation. Companies are spending more than ever to learn where they are vulnerable, to deploy the latest security solutions and to hire the talent necessary for a strong cyber defense. Our research finds that 97% of large firms have undergone audits or assessments of cybersecurity over the past three years, 70% regularly upgrade most of their cybersecurity technologies, and three out of four have senior executives focused squarely on cybersecurity, often a chief information security officer.

In spite of this investment, our research finds that many firms continue to overestimate the effectiveness of their cybersecurity because they fail to grasp the complexity of the challenge. Specifically, many are not developing the long-term strategic capabilities essential for robust cybersecurity. Indeed, most struggle to comply with simple best practices. Only 43% percent of executives believe that their firms follow best practices for cybersecurity, but deeper analysis identifies that only about 24% of firms actually meet that bar. This gap represents a broad swath of executives and companies who believe that they are better protected than they actually are. Meanwhile, cyberattacks are expected to cost businesses $6 trillion annually by 2021, twice the cost of 2015.

Executives overestimate their cybersecurity



Time and again, a familiar pattern emerges in the post-mortem analysis of data breaches: Despite a high level of awareness among senior executives and substantial investments in cybersecurity technology, companies remain vulnerable and these weaknesses are ruthlessly exploited. A key factor in many breaches is that leaders fundamentally misunderstand the characteristics of good cybersecurity, and they underestimate the rigor necessary to achieve it. Consequently, they approach the issue at a tactical level, ticking boxes rather than undertaking the serious work of building deep and strategic capabilities necessary to achieve real cyber resilience.

Identifying common weaknesses

At some level, executives appear to understand the limits of their cybersecurity posture: In a recent survey by security firm FireEye, slightly more than half of respondents don't believe that their organization would respond well to a cyberattack. The concern is warranted. A vast number of things need to work well to achieve cybersecurity resilience, and this complexity can overwhelm executives and misguide their focus *(see Figure 1)*.

The first place they look for solutions is usually technology. Large companies use dozens of products and services to meet their needs, and they invest in policies and standards to ensure that their defenses remain proactive and up to date. The greater challenge comes in ensuring constancy so that policies and standards are applied appropriately across complex global organizations. Even applying simple

Figure 1: A range of common mistakes weaken cybersecurity

Difficulty locating the crown jewels

Some systems are more important and sensitive than others, warranting greater investment in security; cybersecurity experts should be paired with industry experts who can identify the crown jewels

Unfocused spending

Many companies roll cybersecurity budgets from one year to the next, but it's better to reevaluate annually and determine spending based on current threats and business priorities

Ignoring frontline advice

Some companies lack processes to gather input from their cybersecurity teams, but leaders shorten and automate this information cycle to continuously strengthen their security posture

Forgoing the cloud

IT veterans can be wary of cloud-based cybersolutions, but given the security expertise of large cloud service providers, these can be even more secure (and less costly) than on-premise applications

Conflict of interest in reporting

When cybersecurity leaders report to the chief information officer, their recommendations sometimes conflict with other IT priorities; ensuring direct access to the board can help elevate security concerns

Source: Bain & Company

security patches can take large organizations months or even years to achieve, leaving systems vulnerable in the interim. Some large breaches in recent years were because of failures to update web servers against known vulnerabilities.

Technology is only one arrow in the quiver. Because so many cyberattacks start by exploiting vulnerabilities in employee behavior, education is also critically important. Fewer than half the companies we surveyed provide regular staff training on cybersecurity, and, far more surprising, only 55% provide adequate training for their cybersecurity professionals.

Third-party risk represents another common vulnerability, but fewer than half of companies regularly assess the security posture of their suppliers and partners.

Most companies invest in audits to give leaders a sense of the state of their cybersecurity, but audits can also focus on superficial issues and lead to a false sense of security once the identified vulnerabilities are addressed piece by piece. Audits should help verify program delivery and outcomes; they should not serve as the primary input for defining programs or cybersecurity strategy.

Finally, executives struggle to understand how much they should spend on cybersecurity. Reliable industry benchmarks are difficult to find, so a lot of cybersecurity teams try to align their spending with peers based on available information. Most companies just roll their budgets over or add annual increases, but few take a zero-based approach to their cybersecurity spending based on the actual threat environment.

Building mature capabilities

While all of these aspects of cybersecurity need to be addressed, none will build strong resiliency on its own or even jointly. The long-term solution requires redefining cybersecurity as a set of strategic capabilities that can be built and improved over time to continuously address the ever-evolving threat of cyberattacks. Neither technology solutions nor third-party services nor following industry standards can substitute for a fully holistic approach to cybersecurity maturity *(see Figure 2)*.

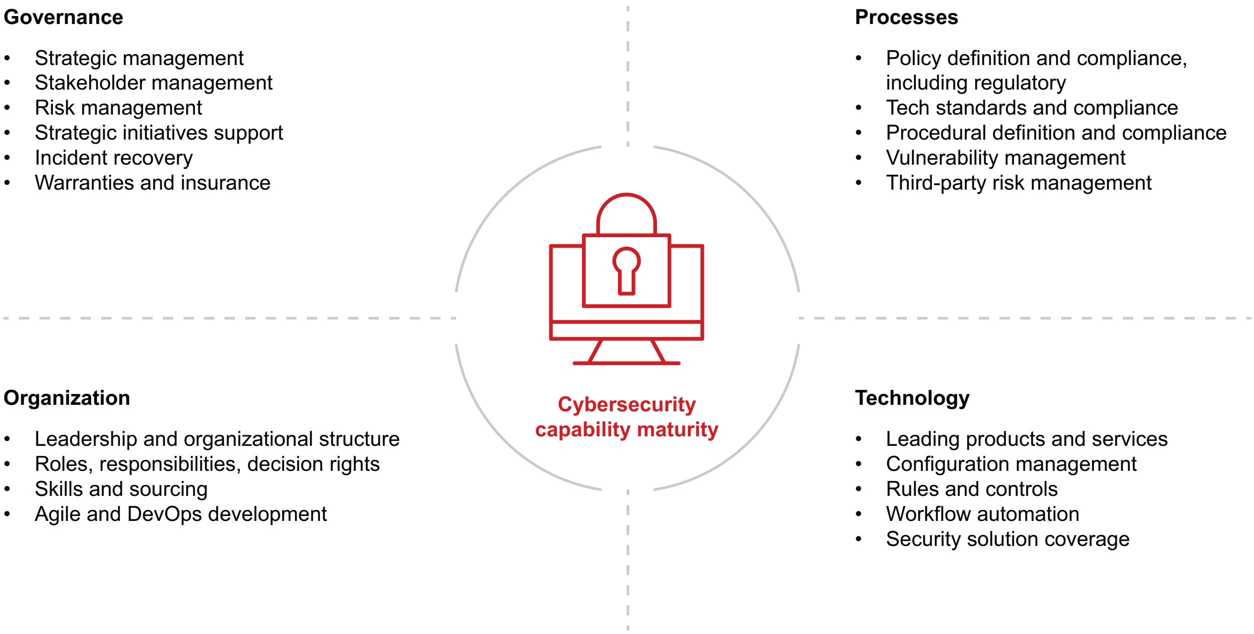
Building up these capabilities to the appropriate level of maturity takes a sustained effort over months or even years, but companies can achieve their cybersecurity maturity goals by following a clear set of discrete steps.

- **Develop a baseline.** Understand where you are starting from by measuring current maturity levels across the full range of 20 capabilities.

- **Identify benchmarks, and determine target maturity levels for capabilities.** Establish the target capability maturity level that is right for your company, and bear in mind that industry, region, critical assets requiring different protections, benchmarks and the current threat environment will all have an impact.

- **Define a roadmap, and begin to follow it.** Address the most critical capability maturity gaps first, especially those that concern your most valuable assets. Then define more comprehensive

Figure 2: To build up their cyber resilience, companies need to develop capabilities in 20 key areas



Governance

- Strategic management
- Stakeholder management
- Risk management
- Strategic initiatives support
- Incident recovery
- Warranties and insurance

Processes

- Policy definition and compliance, including regulatory
- Tech standards and compliance
- Procedural definition and compliance
- Vulnerability management
- Third-party risk management

Organization

- Leadership and organizational structure
- Roles, responsibilities, decision rights
- Skills and sourcing
- Agile and DevOps development

Technology

- Leading products and services
- Configuration management
- Rules and controls
- Workflow automation
- Security solution coverage

Note: Bain's cybersecurity maturity framework incorporates elements from the National Institute of Standards and Technology cybersecurity framework, Sherwood Applied Business Security Architecture, and ISO 27001
Source: Bain analysis

initiatives to enhance capabilities in other key areas. Take on no more than 10 initiatives over an 18- to 36-month period.

- **Strengthen the commitment to continuous improvement.** Reassess capability requirements and maturity levels regularly. Refresh the strategic cybersecurity roadmap to build capability maturity where needed, and ensure that the plan is adequately funded.

Finally, part of continuous assessment is understanding what level of risk can and should be mitigated through cybersecurity insurance. No amount of insurance can cover the damage of a major, highly visible security breach, but insurance is an indispensable component of cybersecurity risk management. FireEye found that half of the companies it surveyed are insured against this type of risk, and another 41% plan to add insurance over the next 18 months.

Taken as a whole, the approach to building cybersecurity capability maturity is a straightforward journey, not unlike other transformational initiatives, but experience shows that it can require sustained focus and a commitment of years to bring capability levels in line with the real needs of the company. The most important step is the first one: Executive teams must come to grips with the scale of the challenge and acknowledge that, in most cases, everything they are doing around cybersecurity is probably not enough. With that understanding, executives can take the necessary steps to increase their cyber resilience to protect their organization, its assets and its stakeholders.

Bold ideas. Bold teams. Extraordinary results.

Bain & Company is a global consultancy that helps the world's most ambitious change makers define the future.

Across 58 offices in 37 countries, we work alongside our clients as one team with a shared ambition to achieve extraordinary results, outperform the competition and redefine industries. We complement our tailored, integrated expertise with a vibrant ecosystem of digital innovators to deliver better, faster and more enduring outcomes. Since our founding in 1973, we have measured our success by the success of our clients. We proudly maintain the highest level of client advocacy in the industry, and our clients have outperformed the stock market 4-to-1.

For more information, visit **www.bain.com**