COLLABORATIVE CYBER DEFENSE

Barriers and Best Practices for Strengthening Cyber Defense by Collaborating Within and Across Organizations

William Guenther, Michael Figueroa, Marc Sorel

MAY, 2018

202 Burlington Road, Bedford, MA 01730 | info@acscenter.org | @ACSCorg | 781-271-5173 |

OVERVIEW

The objectives of this project were to identify organizational models for efficient collaboration on common defense, including collaboration internal to organizations and collaboration with external stakeholders. Researchers worked with ACSC members and other experts, and interviewed CISOs, CIOs, analysts, business leaders and others in a range of sectors including financial services, healthcare and pharmaceuticals, aerospace and defense, high tech, consumer, and government. Through these interviews, and a targeted survey measuring "digital resilience," the project offers a perspective on the most effective cyber collaboration (for example, through the creation and expansion of cyber consortia or utilities); describes the benefits and challenges of institutionalizing informal partnerships and sharing intelligence and best practices; and makes recommendations for enhancing cooperation, which is necessary to address cyber security threats.

Acknowledgments

The ACSC undertook this project with assistance from **Mass Insight Global Partnerships**, and in conjunction with research partner **McKinsey & Company**.

Special thanks to our **National Advisors**:

- Mike Brown, Spinnaker Security (Co-Chair)
- Gary Gagnon, (Co-Chair)
- John McKenna, Liberty Mutual
- Mike Papay, Northrop Grumman

Thank you also to the **organizations who participated in the interviews**:

Blue Cross Blue Shield of MA *
Commonwealth of Massachusetts *
Federal Reserve Bank of Boston *
Fidelity
Liberty Mutual *
Manulife *
MIT Lincoln Laboratory *
MITRE *
MUFG *
Northrop Grumman
RSA Security *
Vertex Pharmaceuticals *

**ACSC Members*

With appreciation to our **research sponsors**:

BENTLEY UNIVERSITY

MUFG

Plus one anonymous sponsor.

And as always, thank you to the **ACSC members**, whose ongoing engagement supports important initiatives and research such as this, which help to build the cyber resiliency of the entire community.

202 Burlington Road, Bedford, MA 01730 | info@acscenter.org | @ACSCorg | 781-271-5173 |

COLLABORATIVE CYBER DEFENSE

INTRODUCTION

Cybersecurity is a persistent and top concern of senior management across industries. The concern is warranted: **Organizations increasingly face more and more sophisticated cyber attackers, with more value at stake, and an increasing gap between offensive and defensive capabilities.** The past few years have been marked by a swell in the number and severity of cyber incidents and breaches. For example, one leading technology company breach disclosures involved billions of records. Others had close to 150 million records breached.

The largest enterprises are at risk, with leading North American institutions in healthcare, financial services, and retail losing 70-80 million records each, but they are not the only ones. Attack volumes for Small and Medium-sized Enterprises in North America are outpacing the F2000, while volumes of attacks targeting North American critical infrastructure increased by >100% year-on-year from 2016. Confidence in the technology sector was shaken by the Meltdown and Spectre vulnerabilities in the processors that underlie the computing behind much of the global economy's critical systems, putting significant swathes of value at stake for leading institutions and demonstrating the persistent gap between offense and defense.

As institutions continue to transform digitally and the number of connected devices expands from 10 billion by the end of 2017 up to ~20.4 billion forecast by 2020, the cybersecurity threat is projected to become more material and more systemic for institutions as threats impact whole industries, not just individual entities.

Unfortunately, despite these trends, organizations often limit their capacity by approaching cyber risk in isolation, as individual organizations against a range of increasingly coordinated attackers, where they are often not the best natural owners of the capabilities they deploy. **There is a missed opportunity for collaborative cyber defense both internally (across departments within an organization) and externally (across vendors and with industry peers) that expands and improves defensive capabilities cost effectively.**

Having assessed in the last 12 months, through surveys and interviews, the digital resilience of a variety of institutions across a range of sectors including financial services, healthcare, pharmaceuticals, aerospace and defense, high tech, consumer, and government, the following emerged as specific opportunities for more effective collaboration:

- Increased sharing of information internally
- External collaborations around vendor security evaluations and the supply chain
- Using simulation exercises for critical training
- Focus on C-suite leadership to deliver fact-based reports on progress and performance
- More collaboration around workforce development

202 Burlington Road, Bedford, MA 01730 | info@acscenter.org | @ACSCorg | 781-271-5173 |

FINDINGS

Overall, the study found that cooperation does happen and is growing, but there are also barriers that inhibit further evolution.

- There is a **strong correlation between collaboration and cyber-security maturity**, indicating collaborative cyber defense is an essential ingredient in an effective cyber program
- **Most collaboration is informal and unstructured**, indicating opportunity for more structured activities and networks.
- **Significant gaps exist between more mature organizations and others**, indicating potential for cross-fertilization of practices.

ACSC participants were most mature in internal collaboration, with the security team managing a complex stakeholder landscape. Internally, enterprises are also increasingly focused on training and skill building across their security team, with more formal career laddering and investments.

Externally, there is still much room for progress. Organizations are increasingly sharing information through informal channels, with growing use of more formal mechanisms, and are exploring opportunities to coordinate on security across their supply chains. There is a broadly recognized need to massively expand the talent pipeline at all levels of experience.

Five primary areas of effective collaboration emerged from the investigation, across both external and internal collaboration.

1. Cybersecurity Governance Requires C-Suite Leadership

Cybersecurity decisions continue to be primarily CISO-driven, with limited engagement by business executives. The primary exceptions are in highly regulated sectors and segments, e.g., financial services, healthcare, and aerospace/defense. The state of maturity continues to evolve, for example in financial services firms, where there is growing involvement by CRO and risk team in cyber governance. For most enterprises, decision-making processes are ad hoc. When an institution considers security beyond compliance, the trend is to view it primarily as a technology problem, instead of critically examining people and process in parallel. This is evolving for many organizations, with increasing recognition that a business-back approach to risk prioritization and an intentional approach for managing insider threat and risk culture are critical to managing cyber risk.

For more than half of ACSC members, the business case methodology for new projects explicitly includes cyber risk assessment in the initial stages, including engagement with the security team, and the company's development methodology explicitly requires an assessment of potential related cyber-security risks and

costs.[1] However, for a large majority of members, the security team role is primarily for review and sign-off, rather than broader engagement on how security can be part of the business value at stake.[2] The technology landscape and related cyber challenges are not standing still, with migration to new platforms (e.g., cloud) requiring changes in operating model.

Organizations are challenged to coordinate the establishment of firm-wide data governance, with business ownership of risk often nominal, and security responsibility effectively left with the cyber team. Instead, accountability/ownership of data security needs to be distributed across business functions. Improving data security and governance is a growing priority for many firms, but progress can be limited. Data management is typically highly fragmented and often tied to the IT system rather than the business owner of the information. When security is engaged, reviews primarily focus on technical controls, which are critical but don't cover the necessary landscape of risks.

A central challenge for a more business-based approach are the **limited mechanisms to measure cyber risks and return on investment for the cyber program.** Better measures are required that provide meaningful transparency into both the current state of cyber risk, and progress toward its amelioration.

2. Information Sharing: Expanding, but Barriers Remain

Information sharing is often bilateral between CISO peers with direct relationships, and relatively informal. It is in some ways overly reliant on personal connections, which raises challenges for sustainability and consistency. There are a growing number of facilitating organizations, typically sector-specific (e.g., Financial Services Information Sharing and Analysis Center, or FS-ISAC), which focus on both best practices and intelligence sharing. Among peer organizations, information exchange is typically regularized, but not continuous or real-time.[3] For a minority of firms, both internal and external sources are integrated to provide a combined perspective.[4] Recognizing the opportunity for improvement, there is a growing commercial cyber intelligence market, although **with more data available, effective and timely data analytics that drive toward actionable insight becomes even more important.**

Barriers to increased information sharing include concerns that cyber practices are considered proprietary IP, an ironic side effect as security becomes recognized as a source of differentiation and competitive advantage. There are also concerns about inadvertent sharing of personally identifiable information, or PII, while trying to coordinate threat analysis and response. Organizations can encounter delays and friction when trying to address these challenges, driven by the complexities of negotiating nondisclosure agreements and other legal frameworks, and the operational time-lag in sharing threat reporting, which reduces the value of intelligence data and the incentives to share. The need for a unified threat and risk profiling for potential adversaries, vulnerabilities, and threat vectors is unmet; the regular collection of threat and risk data and breach statistics remains an unrealized opportunity.

[1] McKinsey Digital Resilience Assessment

[2] McKinsey Digital Resilience Assessment

[3] McKinsey Digital Resilience Assessment

[4] McKinsey Digital Resilience Assessment

3. Third-Party Security Evaluations: A Collaborative Opportunity

Nearly universally, **respondents recognized that tremendous duplication in security evaluation of vendors and third parties occurs across companies**, presenting opportunities for gains in both efficiency and effectiveness. And the problem is **increasingly more critical to solve, given the implicit concentration of risk through shared cloud vendors.**

Most organizations use similar but different evaluation frames, driven in part by third-party standards (e.g., CSA STAR), though the evaluation process itself is completely internal for a majority of ACSC members.[5] As with information sharing, there are some sector-specific facilitating organizations (e.g., CyberFit for healthcare firms) to coordinate and share evaluations. Even when organizations want to collaborate, they face coordination challenges aligning on shared criteria, given the variations across enterprises and the perceived need for firm-specific and tailored evaluations. Some question the value of the evaluations themselves, seeing limited value from interrogatories or even site visits. And as with information sharing, there are limited venues and formal organizations to coordinate activities.

4. Workforce Development: A Major Challenge and Collaborative Opportunity

On the talent front, all organizations are facing a significant shortage—the "missing million" cyber professionals that are needed to meet demand. And when talent crosses the threshold and a candidate is being considered, organizations face a limited ability to identify candidates with necessary skills. The talent market is highly competitive and fragmented. While there are some partnership programs between enterprises and academia, they tend to be bilateral and university-specific, and are unlikely by themselves to respond adequately to the scale of the challenge.

The entry point challenge is particularly severe. Given the natural preference of enterprises for experienced candidates, even highly motivated candidates can be challenged to get the first couple years of experience that will give them more credibility and effectiveness.

5. Simulations: An Increasingly Important Training Opportunity

Internally, organizations are moving up the maturity curve in cyber decision making, with a broader and more senior range of stakeholders involved in a meaningful way. Given the unfortunate inevitability of negative events, increasingly realistic simulation "war-game" exercises are becoming part of business as usual. With data at the heart of what attackers are seeking, and what organizations are looking to protect, security needs to be integrated into data management. Participants reported that they can effectively identify and prioritize "crown jewel" assets and deploy active defenses focused on that subset of data, though most business leaders view themselves as participants in the process, rather than as driver or owners of prioritizing critical data and risks.[6]

[5] McKinsey Digital Resilience Assessment

[6] McKinsey Digital Resilience Assessment

More broadly, cyber governance needs to be clarified, with better understanding of roles and responsibilities within and beyond the security team. Including all key players in simulations addresses this need.

Most organizations are augmenting their incident response plans with live simulation exercises. Most common are single-firm war gaming exercises, with some cross-functional players from business, legal, and public relations, usually focused on table-top simulations for cross-function exercises, while IT/security-only war games tend to be more technical. In financial services there are some examples of multi-firm scenarios, such as the Hamilton series organized by the U.S. Treasury. In general, preparedness and response are not yet viewed as a baseline expectation of all participants' roles, but rather as a "plus." **Currently, a minority of organizations leverage external partners to improve incident response.**[7] One key consideration in incident response planning and practicing is the need to protect confidentiality of sensitive information during the exercises and live incidents themselves.

CISOs looking to drive a more cross-functional rehearsal can be challenged to get senior participation. With competing priorities, and absent a high-profile incident, engaging the business can face obstacles, even more so in the absence of leadership from the C-suite and the Board. There has been some innovation in technology platforms that can support such simulations, though they tend to focus on simulating the technical breach and response, rather than the business aspect. While there is some interest in cross-sector exercises, the lack of clear conveners outside the public sector makes coordination more difficult.

[7] McKinsey Digital Resilience Assessment

HALLMARKS OF EFFECTIVE COLLABORATION

In addition to the five opportunities for enhanced collaboration, the study identified hallmarks of effective collaboration, both internally and externally.

1. External Collaboration Hallmarks: Active Engagement in Regional Community

Individual firms that are effective at external collaboration share common hallmarks and behaviors.

Leading organizations **work with their peer communities**, with the security team engaging with both sector-specific and cross-sector forums for sharing best practices. The most advanced firms participate formally in one or more joint organizations, with activities ranging from effective sharing, to collective intelligence gathering and distribution, to joint vendor evaluation and contracting.

The most collaborative enterprises are also **actively engaged in the local academic community**, to align curricular priorities and augment the talent pipeline through internships and other programs, participating in research sponsorships and partnerships to advance cyber security knowledge and techniques.

For sustainability, effective organizations formalize their external collaboration and **assure that personal trusted networks are institutionalized**, with clear owners for engaging partners, which can enable new players to "slot in" as organizations and communities evolve. There needs to be explicit responsibility for engaging both customers and vendors to identify security needs and collaboratively develop solutions. For nearly all enterprises, responsibility for coordinating security across the supply chain lies with the cyber team.[8] For leading organizations, explicit attention is given to ensure security improvements do not introduce unnecessary friction into business operations.

2. Internal Collaboration Hallmarks: Driven by the C-Suite

Internal collaboration across functional groups was identified as critical to effective cyber security management. The mandate to do this effectively comes from the top.

Effective internal cross-functional cyber governance **requires a cyber security committee at the enterprise level**, with leaders beyond the IT and security teams, usually consisting of senior executives that represent the core business, HR, privacy, and compliance, at minimum. Given the data-centricity of the threat landscape, clear data and risk ownership by the business, with established roles and responsibilities for data stewardship and governance, were demonstrated by leading organizations.

Effective collaboration is enabled by a **strong, top-down cyber mandate**, with support for improved cyber security explicitly endorsed by the board and senior executives that recognize the business value of digital resilience. Translating that senior support into action requires **consistent enterprise-wide policies**

[8] McKinsey Digital Resilience Assessment

and standards that internal and external programs are expected to meet in a timely and cost-effective manner.

This is supported by **embedding cyber team members across the operating model** to promote engagement across departments and business units. For most organizations, security team members are regular but episodic participants in business processes, rather than being fully integrated end-to-end.[9]

Cyber-mature organizations tie investments to top cyber risks, with security investments and budgets driven by business-back prioritization, grounded in structured and consistent evaluation of cyber risks. The best firms start by knowing what they have, what matters most (i.e. which applications and systems), and subsequently spending to secure them across the value chain from identification to post-acquisition growth strategy. Dedicated cyber security resource commitments are guarded against alternate demands and diversions, increasingly difficult as IT budgets are challenged and constrained.

For mature firms, **cyber team members are involved in key procurement and product development** decision making and processes.

Active cyber risk culture management was viewed as a critical part of the security program for advanced organizations, with recognition that insider action, intentional or accidental, is the source of half or more of cyber security risk exposure. Cyber awareness and action needs to be viewed as part of everyone's job. Currently about half of organizations have a formal program, while for others it is informal or ad hoc.[10] At a baseline, cyber policies are tailored to organizational objectives and are embedded into HR and IT policy and programs, while for more sophisticated enterprises there is strong integration with risk and safety.[11] Leading organizations have established training and awareness programs, including phishing campaigns and incentives for individual and group performance.

[9] McKinsey Digital Resilience Assessment

[10] McKinsey Digital Resilience Assessment

[11] McKinsey Digital Resilience Assessment

OPPORTUNITIES

Solutions to enhance collaborative cyber defense must encompass peer groups, internal stakeholders, and the broader set of external partners.

Improving collaboration with internal stakeholders, external peer groups and third-party partners can have a positive impact on cyber security maturity. Organizations should consider what collaboration opportunities might be advantageous individually and collectively. Part of sustaining opportunities for collaboration internally is **establishing governance structures and operating models that encourage interaction** between cyber teams and other business units, and externally by **increasing data sharing on threat factors, incidents, and breaches.** Enterprises should share governance and operating model choices that work for them as individual institutions, and discuss what effective practices might make sense to share in an anonymized fashion.

Specific opportunities for improving an organization's cyber resilience include the following:

1. Public-Private and Cross-Sector Simulations

One of the high-potential opportunities is to conduct **multi-organization crisis response exercises with peers, to develop "muscle memory" for managing cyber incidents and strengthen joint response**. These can and should focus on cross-functional coordination challenges, since typically as much harm comes from non-technical response as from the underlying technical breach. Participants recognized there would be more value from regular series of exercises, covering a range of scenarios over time, rather than from a one-off event. Currently, about half of ACSC members have participated in a joint war-game

simulation.[12] **These can become even more valuable with engagement of the state and federal government.**

2. Threat Intelligence Sharing and Shared Analytics

Sharing of threat intelligence and analytics capacity is particularly valuable, and can be enabled by developing common standards for exchanging information, and disseminating best practices for managing legal and regulatory risks. Beyond the walls of the organization, **there are opportunities to promote changes in public policy to reduce barriers to information sharing,** for example by creating safe harbor provisions or facilities that address legal and compliance concerns.

3. Effective Practice Sharing

There are significant opportunities in expanding the opportunities to share effective practices.

Research

Organizations can promote the dissemination of best practices through formal research projects and publications, beyond current informal networks and relationships.

Example: Establishing **mentorship programs** for CISOs, heads of cyber risk, and their teams to accelerate learning and relationships.

Internal Effective Practice

Internally, organizations need to **facilitate cross-functional governance of cyber risk management** by identifying and implementing best-practice structures and processes to engage across IT, risk, business, legal, and cyber security leaders. Risk management processes need to have clear business value and avoid creating undue friction or delays, and business leaders should take more active ownership of cyber security risks given potential existential exposures. **Fundamentally, business teams need to be accountable for security and risk management.**

Just as multi-firm war games can improve readiness, individual companies should **regularize cross-functional crisis response exercises** to stress-test cyber readiness among the executive team in advance of an actual enterprise-scale incident.

Evaluating and actively **managing cyber security risk culture** needs to go beyond increasingly standard phishing exercises and mandatory trainings, with **systematic risk culture benchmarking**, and advanced insider threat analytics practices to reduce false positives and increase the effectiveness of interventions.

[12] McKinsey Digital Resilience Assessment

Metrics and Performance Evaluation

With Boards and senior executives showing an increasing appetite for addressing cyber risks in a rigorous manner, there is a need to disseminate and leverage methodologies for evaluating, quantifying, and prioritizing cyber risks to support more compelling business cases to guide investment decisions. At a baseline, there needs to be **regular reporting on cyber metrics to C-level executives and the Board**, recognizing that this is an area where there is still debate as to what to track.

Effective cyber risk reporting embraces both business measures (e.g., value at risk, experienced losses) and technology metrics (e.g., percentage of attacks stopped at each step across the "kill chain"). Dashboards should encompass metrics that are both trailing (e.g., employee credentials stolen) and leading (e.g., vendors out of compliance on security requirements). The metrics should be selected, and thresholds set, with an eye to driving decision making (e.g., for cyber investments).

Third-Party Security Evaluation

Up and down the supply chain, there is an opportunity to establish **standardized and potentially shared security evaluations of third parties** to improve effectiveness and efficiency of vendor risk management.

Example: As the IT landscape evolves from in-house and on-premises to cloud computing, there is an urgent opportunity to address the implicit concentration risk stemming from common cloud vendors through multilateral, rather than bilateral, information sharing and incident response coordination.

Reviewing security technology

Given the proliferation of security technology, collecting and sharing experiences with security technology vendors, and leveraging the experiences and learnings from individual enterprise engagement, can help inform better decision making on adoption. At a base level, **mapping ecosystem and range-of-vendor offerings, and sharing best practices on defense technologies can help clarify the landscape** and identify meaningful options. There is potential to work with industry peers to develop common criteria for security vendors, and more deeply involve the internal security team in proposal processes.

Working with Educational Institutions and the Community

Organizations can collaboratively address the cyber talent challenge by working with educational institutions and non-profits to **establish effective cyber curricula** that fit ever-evolving needs for new skills to address evolving threats, fostering cyber talent by participating in and **facilitating co-ops**, **internships**, and other hybrid experience programs with universities, and **sharing best practices on training and supporting cyber career paths within organizations.**

In the broader community, educating citizens and customers to convert them into active allies and co-defenders improves collective security. Sector-level efforts can share common messaging (e.g., financial services around identify fraud), and public-private partnerships can help inform the broader community (e.g., as part of common civics education in school).

ACTION

Looking to the future, the ACSC and its members can prioritize several initiatives to enhance collaborative defense among its member organizations, the community, and the region.

1. Multilateral Public-Private War-Game Simulations

An annual multilateral war-game simulation with state and federal collaboration can further the region's position as a leader in cyber security, enhance the region's capabilities for responding to shared threats, and influence the national and international dialogue on cyber crisis response. The exercise would have the most impact by **approaching the breach event as a business challenge**, rather than a technology problem.

A joint exercise, with involvement from the public sector, would allow members to practice the collaboration with other firms, test information-sharing across institutions (including identifying and extending communication channels), and check if internal speed of reaction and current plans are sufficient to contribute productively to crisis response. The potential is to establish a series of exercises, which will also expose other opportunities to collaborate beyond the games. Also, beyond the exercise itself, it would allow the ACSC and its members to shape the cyber agenda, identifying improvements needed for interaction mechanisms and protocols (e.g., regular joint war-gaming), and shape the regulatory agenda and communication, influencing supervisory and regulatory expectations and building interfaces of firms with regulators.

2. Cyber Governance: Boards and the C-Suite

The ACSC can also improve cyber governance by identifying and disseminating best practices for security teams collaborating with their boards and senior leadership. This can include board-focused versions of incident response simulation, developing and promoting best-practice governance archetypes, and collating and distributing effective ways to evaluate and even quantify cyber risks, to better connect cyber decision making into corporate governance.

3. Third-Party Security Evaluation Clearinghouse

Across the supply chain, the ACSC can establish a clearinghouse for third-party evaluations, reducing duplication across members, and accelerating the pace of commerce. While there was some interest in aligning on a shared evaluation questionnaire set, the consensus was that the problem was not the shortage of third-party standards, but rather the lack of coordination and unnecessary duplication of evaluation and review processes.

4. Public-Private State Agenda on Workforce Issues

Finally, the ACSC can support the Commonwealth's new Cyber Center at MassTech initiatives, and continue to collaborate with universities to develop public-private programs addressing workforce issues (the "missing million" cyber professionals) by facilitating and supporting public-private partnerships, and partnerships between enterprises/academia/nonprofits, to shape effective cyber curricula and develop meaningful experiential learning that create and accelerate professional opportunities.

About the Authors

Bill Guenther is Chairman, CEO & Founder of Mass Insight Global Partnerships, and Chair of the ACSC Board

Mass Insight Global Partnerships (MIGP), founded in 1989, organizes strategic leadership groups connecting university, industry and government partners to shape public policy and drive breakthroughs in talent, innovation and regional economic development. Its major current initiative is the *Boston Financial Services Leadership Council*, which brings together financial services senior executives and academic partners to develop partnerships supporting the digital transformation of the sector. Mass Insight also provides consulting services to the *Advanced Cyber Security Center* which it launched as an independent nonprofit in 2011. www.massinsight.com.

Michael Figueroa is the Executive Director of the Advanced Cyber Security Center

The Advanced Cyber Security Center (ACSC) is a member-driven non-profit that harnesses the power of collective resources to strengthen cyber defense, develop security talent, and advocate for well-informed public policies. www.acscenter.org

Marc Sorel is an Associate Partner at McKinsey & Company, and General Manager of McKinsey Cyber Solutions

McKinsey & Company is a global management consulting firm that serves a broad mix of private, public and social sector institutions. For almost a century, McKinsey has helped clients make significant and lasting improvements to their performance to realize their most important goals. www.mckinsey.com