ZERO TRUST AND BEYOND

A Summary of 13 Roundtable Dialogues Conducted by Billington CyberSecurity

In 2022, Billington Cybersecurity hosted 13 Innovation Round Tables (IRTs) consisting of senior public/private sector cyber experts discussing specific key areas of cybersecurity in Chatham House Rule format (for a complete listing of the IRT topics, see the appendix). The overall results of these discussions offer very valuable lessons to people interested in moving cybersecurity forward, highlight lingering issues that impede its advancement, and suggest areas where more attention is needed to further its development.

Below is a high-level summary of the findings:

- The need for the entire community to **embrace zero-trust (ZT) as a framework** in order to reduce risks associated with
  - an increasingly mobile and remote workforce,
  - increased demand for connectivity with other organizations and consumers,
  - tighter integration between business and operational networks and,
  - agile adversaries who adjust their tactics to leverage this increased surface area.
- That the challenges to move to a ZT framework are less about current technology and methodology, and more organizational and definitional in nature.
- **This implies that ZT can be achieved now** by taking incremental steps with a focus on:
  - picking several key objectives,
  - identifying, and garnering the right talent,
  - building a better understanding between technologists and mission leadership, and
  - increased user awareness of basic cyber hygiene which will also push the culture changes needed to accompany it.
- That **having a sound cyber resiliency plan** in addition to embracing zero-trust can better ensure overall cybersecurity, and
- That more and better **public-private engagement** can significantly improve adoption of the ZT framework as well as lead to an overall national reduction in cyber risk.new technologies. Group discussions centered on five key areas to help build both public and private entity continual trust verification environments; one that prioritizes prevention but is prepared to identify and respond should bad actors find a way to intrude.

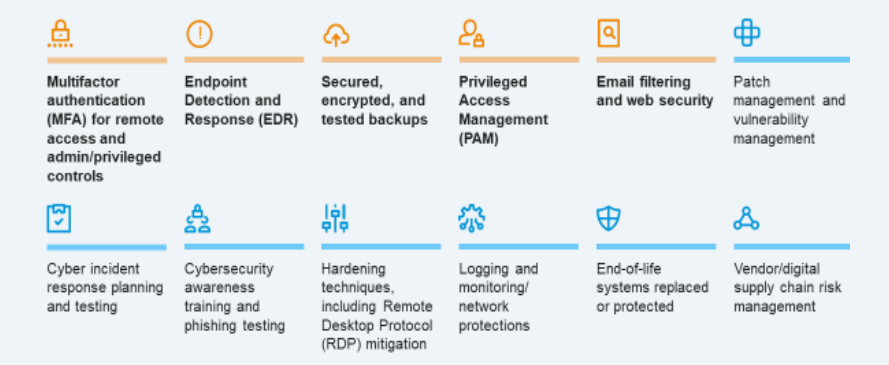
ZERO TRUST FRAMEWORK

The IRTs highlighted that embracing and deploying a ZT framework is imperative to achieve better cybersecurity across both the public and private sectors.

Put simply, Zero Trust focuses on the need to continually authenticate and validate whether users, applications, or processes have a legitimate right to access and do the things they want to do on any given controlled and managed digital environment—whether that environment be a single network, an amalgamation of clouds, or multiple networks controlled by a singular entity. The groups agreed in principle that key requirements for those responsible for cybersecurity for any given trusted security digital environment should be to:

- Implement strong controls that are optimized to protect against known cyber risks. According to industry leaders who continually work with a multitude of different private sector clients, the top controls to consider are:

Top cybersecurity controls are the key to risk mitigation, resilience, and insurability.



Source: Marsh

- Have a full knowledge of what and who is operating within their trusted security digital environment and how they operate.
- Have a full and dynamic knowledge of the environment's activities via monitoring. According to a new McKinsey study, over the past three years, companies have boosted their share of what they log from about 30 percent to about 50 percent on average and are pushing toward 65 to 80 percent over the next three years.
- Have defined and enforceable rules and policies that spell out what should be happening within that environment.
- Have a process that identifies questionable behavior both as it comes at your environment and from within, and
- Have a process and system that can be continually updated as the above things change, and as new types of threats arise as adversaries alter their tactics and tradecraft.

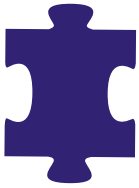
KEY ISSUES FOR ADOPTION

Many participants acknowledged that today's technology, information science, known processes, and procedures offer means to fully implement a zero-trust environment today. Most agreed that both federal and private entities are thinking about how to adopt a ZT framework and many have already designed, partly built, and procured things necessary to achieve it. Much of the discussion across all the IRTs focused on the question:

"IF WE HAVE IT, WHY HAS IT NOT BEEN ADOPTED?"

The groups pointed to several ongoing challenges faced by all that include:

People continue to have a hard time figuring out what they should protect, who is responsible for protecting it, and how to stay knowledgeable of what needs to be protected as their environments change.



They cited such key challenges as: correctly labeling and classifying data, the lack of sufficient resources, and the myriad of real-life things that cybersecurity professionals have had to deal with such as Covid, demand for where people work, and the growing surface areas that they must deal with such as satellites, IoT and the growing connectivity between IT and OT worlds.

Organizations continue to struggle to strike the balance between achieving their mission versus protecting it.

IT and cyber decisions continue to be outside of organizations' business decision process. Cyber decisions are often not tied to an organization's overall mission due to business owner ignorance or failures in adequate communication. This leaves cyber decisions strictly in the hands of cyber professionals who are left to guess how cybersecurity fits into the larger strategic picture.

The lack of a cost/benefit analysis to effectively measure cybersecurity's impact.

A lack of the "right" cybersecurity workforce—whether in house or outsourced—to move the program forward.

IDENTIFIED STEPS
TO MOVE BEYOND THE CHALLENGES

The Round Table discussions also provided plenty of excellent ideas to counter some of these key challenges and move cybersecurity programs forward. Group discussion highlighted that:

Create a Plan.

Perhaps the simplest and yet most effective way to embrace zero-trust is to start the journey. Group discussion focused on building and implementing a plan of action that focused on picking a singular path, and working to achieve small, incremental steps that included overall organizational workforce training and education via repetitive processes.

Close the Knowledge Gap.

Finding ways to elevate cybersecurity into the boardroom and building regular interaction between the CISO, CIO, and corporate management to sync cybersecurity with an organization's key missions and goals. The CIO and CISO must make it a priority to close this knowledge gap to ensure that technology and security decisions align with organizational priorities. This effort should include building a regular process of communicating corporate mission and goals to the cybersecurity workforce while finding ways to make cybersecurity relevant to all users.

Picking a single approach.

Focusing on a singular strategic approach can help better prioritize efforts while moving the entire process forward. Once the analysis is conducted, picking a prioritization scheme focused on protecting that which is most important from a business perspective. The group highlighted three examples of strategies to be considered: one focused on managing access through identity, one focused on classifying and protecting data, and one focused on proactive incident management and resiliency.

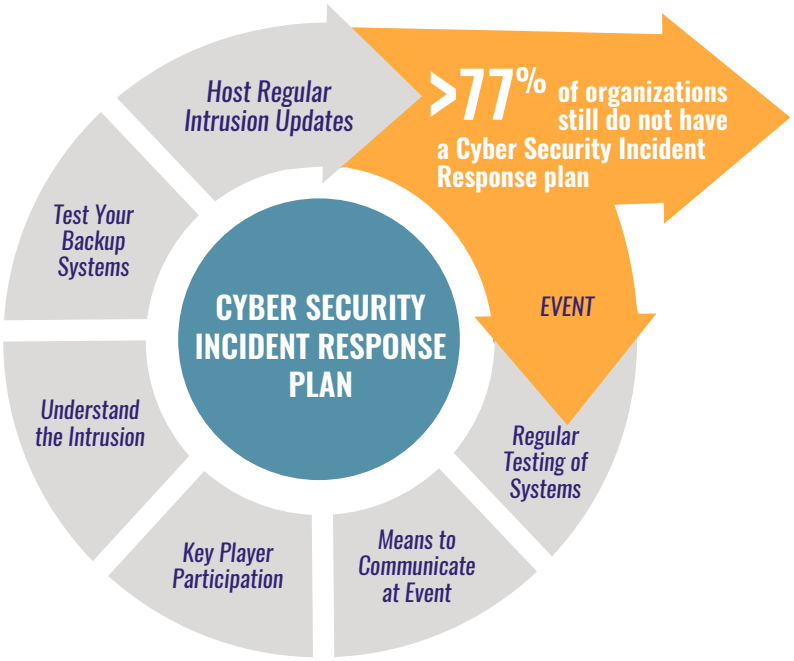
Identifying the "Right" Skillsets.

Taking the time to focus on Identifying the right cyber skillsets needed and developing an approach to acquiring them—either via developing your own work force or using managed services—is time well spent. The group agreed that simply throwing bodies at the problem was not the answer and that more careful planning would go a long way to advance the overall effort. Careful planning should include:

- Assessing the surface area you are currently monitoring and need to monitor to get an overall better perspective of what you might be missing.
- An assessment of current cyber skillsets matched up to current knowledge of the security technologies being leveraged.
- Identifying areas where skill diversity–data analysts, data science, Security Operations officer, etc..,--could be better used.
- Factoring in the deployment of new technologies–such as cloud migration, or the use of multiple types of clouds– as it relates to current available skills.

BEYOND ZERO TRUST:
A CYBER INCIDENT MANAGEMENT PLAN

There were other key cybersecurity topics that the groups discussed beyond zero-trust. One of the continual themes focused on the need to improve cyber resiliency and in particular the need to build a strong cyber incident response plan. According to a recent study undertaken by the cyber training company, Cybint, more than 77% of organizations still do not have a Cyber Security Incident Response plan.



The group agreed that everyone should have a cyber incident management plan that includes:

- Regular testing and practice to make it stronger, up to date, and in sync with an organization's mission focus.
- A means to communicate securely during an event, given the potential that the system will be impacted during an event.
- Key player participation during practice to include operational leadership.
- Having a process that allows you to first understand the intrusion-its scale, its likely intention, its functions, etc.--so that you can include facts that can help make important operational decisions during the event.
- Testing your back-up systems that could be leveraged should intruders incapacitate your active network.
- Hosting regular briefings of what is happening as events unfold to try and keep everyone up to speed.

PUBLIC-PRIVATE
COLLABORATION & INNOVATION

Additionally, there was a lot of discussion about finding ways to increase the interaction beyond information sharing between the public and private sectors. Group discussion focused on areas that could help overcome common issues, spark innovation, and collectively improve cybersecurity as a team sport. Good ideas springing from these discussions included:

Better leveraging new technologies such as the cloud to improve shared research and development efforts between government and private entities. The group felt that combining this agile build, test, breakdown, rebuild test development cycle could be used to satisfy joint requirements more quickly.

Re-thinking the notion of contracts and how they work to foster improved innovation and provide faster adoption of cybersecurity actions.

The private sector encouraged the Federal Government to get more involved in developing the next international technology standards process.

Overall, these discussions clearly highlighted the need for continued dialogue between the public and private sectors to both better understand and leverage the knowledge inherent in each.

Multiple people involved from both sides have asked to find ways to continue the conversation citing the value of better understanding, continued relationship development, and healthy debates about specific cyber related topics as key to their continued progress as cybersecurity professionals.

Appendix
The 2022 Billington Innovation Round Tables
February 2 – Understanding Your Network Leveraging the Right Data
March 17 - Defining policies for user access, data controls, system mgt responsibilities
April 18 - Building the Right Cybersecurity Controls
June 15 - Managing your Cyber Incident
September 7 - AI/ML Use on Cybersecurity
September 7 - The Role of Quantum and its Impact on Your Cybersecurity Programs
September 7 - Guarding Your Network From the Inside
September 7 - Exploring Ways to Improve Cyber Resiliency
September 8 - Cyber Threat Intelligence
September 8 - Finding, Recruiting, and Retaining Talent
September 8 - What will make a good SBOM and HBOM? How do you ensure better trust in the software that is built and used?
September 9 - Identifying Ways to Improve the Expression of Need between the Public and Private Sectors to Move towards Zero Trust

For a more in depth understanding of each Innovation Round Table and their discussion points, please go to the Billington Website at https://billingtoncybersecurity.com/blog.