Preparing for a Bad Day – The importance of public-private partnerships in keeping our institutions safe and secure

Thomas J. Harrington

Today's cyber threat landscape is evolving at a rate that is extremely aggressive, and attacks are becoming more complex and targeted. Cyber criminals are growing increasingly more sophisticated and harder to predict, the number of connected devices is increasing exponentially, and the growing reliance on the cloud-based systems potentially opens up new attack surface for our cyber adversaries. These factors mean that today's defense techniques and strategies will need to evolve with the threat in order to keep our institutions and information safe and secure. In today's interconnected world, no single entity or organization has full visibility into the threats that exist, and the existence of partnerships, including between the public and private sectors, is extremely important and necessary in protecting us all. As a private institution, we recognize the need to, in a privacy protective manner, build strong relationships beginning with our internal teams and with our critical partners, such as government agencies, the military, and our business partners and clients, all working as a strong network to achieve the common goal of defending against bad cyber actors.

At Citi, our philosophy to keep our firm safe is built on investments in talent, teamwork, and technology. These pillars are critical in supporting our intelligence-led, threat-focused organization and helping us prepare for a *bad cyber day*. Talent management and development are extremely important when thinking about the future of an organization. Our financial community strives to recruit, hire, train, develop and retain talented colleagues to help give us any advantage possible to gain the high ground on the cyber battlefield. We are focused on transforming our workforce by investing in top-level cyber intelligence and Information Security talent from the private and public sectors, as well as from academic centers of excellence.

Thomas J. Harrington is Citi's Chief Information Security Officer. Tom retired with 27 years of law enforcement and national security experience. Mr. Harrington was the former Associate Deputy Director for the FBI and is a recognized leader in the global law enforcement and intelligence communities.

Our mission to recruit and retain top talent spans from recent college graduates with cutting edge training, to seasoned professionals from various backgrounds. These backgrounds include information technology specialists, information security specialists, intelligence analysts, communications specialists, and even those with political science backgrounds. Teamwork is a value that is essential for any organization regardless of size or function.

In an institution as widespread geographically as Citi, teamwork and the elimination of operating in silos is not just of high importance, but the protection of our assets depends on it. Each member of our team must recognize that the advanced adversaries are demonstrating growing sophistication, speed and responsiveness to our changing defense posture. These adversaries are well-networked and sharing knowledge and experiences at a rapid pace. We are focused on implementing leading management practices and initiatives to maximize collaboration, learning, and innovation across functional areas.

To be successful, each day we must demonstrate an ability to learn and share with a wide internal and external audience in a way that empowers them to act positively to safeguard our organization. We are also focused on deploying innovative technologies to secure the business and identifying disruptive technologies that enhance safety and security. We are developing information-sharing platforms, intelligence products, and operational playbooks that inform executive action and decision-making. Our ultimate goal is to evolve our information security programs real-time knowledge of threats and our posture against those threats—in order to prevent, detect, and when possible predict attacks, make risk decisions, optimize defense strategies, and enable action in response

to those threats. Firms across industries, including financial services, must develop a successful battle rhythm focused on information security.

Critical to any organization that wants to achieve an upper hand in the cyber battlefield is the ability to attain what we and our military partners call *Situational Awareness* or commonly referred to as SA. In order to achieve a constant state of SA, Citi is taking steps to create a Cyber Common Operational Picture (COP). This will allow key leaders to have a real-time view of what is happening in the cyber realm, whether it's in the middle of a cyberattack or steady state operations, it is highly critical we maintain a holistic view of the cyber problem set.

Just as the military trains its forces to operate on battlefields against an asymmetric adversary, Citi depends on proper training and constantly exercising to ensure we build muscle memory into our own Standard Operating Procedures (SOPs) or playbooks. We recognize that having sophisticated technology and skilled talent is only half the battle with staying one step ahead of our adversaries. As a result, Citi has taken a proactive approach in achieving the other half by continuously and deliberately testing plans, validating capabilities, and identifying areas for improvement.

In today's interconnected world, no single entity or organization has full visibility into the threats that exist.

Ensuring a good defense is in place requires an organization in concert with one another, to incorporate several key elements when faced with an ever-evolving cyber adversary. Neither Citi nor any other organization can be prepared to defend itself without proper training and exercises. As with soldiers going into a combat zone, firms must train and exercise its cyber talent using a similar methodology used by the Department of Defense (DoD) and Department of Homeland Security (DHS)—*Train, Plan, Assess, Educate, Improve, and Train.* By employing this methodology, companies like Citi can conduct custom cyber-focused exercises that meet organizational objectives.

A key component of our exercise program is the *train up* piece—while not everyone at Citi has a key role or responsibility when it comes to a cyber crisis, it is important we constantly train our business staff to understand and provide a general understanding of Citi cyber capabilities and threats. Outside the mandatory annual information security training all employees must complete, our exercise team conducts *pre-exercise* training to exercise participants and observers. Doing this ensures that *non-cyber* functions and roles within Citi are afforded an opportunity to become familiar with *Cyber at Citi* and provides them an understanding of exercise expectations. As part of the exercise methodology, we then move into the Planning Phase, which is perhaps one of the most crucial elements.

Citi employs a core planning team concept when it comes to planning the exercise scenario. In order to make the exercise realistic, our team works with various internal partners to ensure the scenario is robust and realistic. Our end state goal is to make the exercise as immersive and real, as if participants were actually in the crisis real-time. This is done by creating real world exercise artifacts, such as news video clips, media reports, FBI and DHS reports, phone calls, emails, and social media postings. Over the last year, we have invested significant time and energy into building cyber incident response playbooks that serve as a baseline for notification authorities.

As with any plan or playbook, it has little to no value unless it is tested and exercised on a routine basis (scheduled or unannounced). Over the past few years, Citi has and continues to lean forward with setting the example by instituting a formal cyber exercise program. Not only have we started our own program, but we have also encouraged and assisted other banks and our clients to do the same. We know that building our internal capability and strengthening our cyber readiness posture is crucial to our individual success as a firm, but also recognize we—as an industry—must work together to ensure safety and security of the US financial ecosystem. Citi does this by consistently partnering with global government agencies, including domestically the U.S. Treasury, U.S. Cyber Command (USCYBERCOM), the Army Cyber Institute (ACI), the Naval War College, the DHS, the Federal Bureau of Investigation (FBI), and the Financial Services-Information Sharing Analysis Center (FS-ISAC), to plan and execute critical private-public sector information sharing cyber exercises.

To ensure the safety and security of our institution and industry, it's imperative for us to focus on becoming true learning organizations.

To ensure the safety and security of our institution and our industry, it is imperative for us to focus on becoming true learning organizations. We must prioritize the education and training of our employees and constantly transform andadapt to keep up with bad actors and emerging threats. All of Citi's training exercises are followed by After Action Reports and Improvement Plans that require actionable changes by our businesses.

While we stretch our imaginations to anticipate what our adversaries have in mind for their next attack, we can and will build upon our arsenal of cyber capabilities and resources. By applying our resources, internally and through our external partnerships, we can develop an intelligence-led approach to predict, prevent, and successfully respond to cyberattacks we may face. It is crucial that we continue to develop our staff to think *left of boom* to detect potential threats and properly respond in a timely fashion using documented and tested processes. We must also, in a privacy protective manner,

continue to enhance our public-private sector information sharing mechanisms with our external partners like the military and US government agencies to ensure we all receive actionable and timely intelligence to make informed decisions and take appropriate actions. Most importantly, we must all be continuously learning and adapting our talent, tools, and technology to the ever-evolving cyber threat landscape.

This article reflects the views of the author and should not be viewed as representing the views of Citi nor the FBI. The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.