A Technology Blue white paper

High performance cyberspace security

Improving operational response to cyberspace threats

High performance cyberspace security

Improving operational response to cyberspace threats

Leading organizations are investing heavily in cyber security technologies and solutions to mitigate the risk of cyber attack. Yet unfortunately many are just getting started. Failure to close gaps in cyber defenses soon enough could result in catastrophic level events that threaten the continuity of a business.

"Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation."

- *2010 National Security Strategy*

Introduction

From a technology perspective, cyberspace is defined as the global network of interdependent information technology infrastructures, telecommunications networks and computer processing systems. From an individual perspective, cyberspace is how ideas are exchanged, information is shared, business is conducted, games are played and people are connected. Yet despite immense opportunity, cyberspace, as described in our Nation's 2010 National Security Strategy, enables "one of the most serious national security, public safety, and economic challenges we face as a nation."

Over the past 10 years the number of people around the world connected to the internet has increased from 360 million to over 2 billion, and this trend is expected to continue at an exponential rate into the future. Collaboration is occurring at a rate like never before, innovative creations are improving quality of life, and opportunity is made available where once it was not. Unfortunately those same opportunities are readily available to those with malicious intent as well.

The United States critical infrastructure that enables our quality of life – energy, banking, finance, transportation, communication and defense all rely on cyberspace. Countless ideas, monies, information and communications flow through cyberspace every second. And with widespread availability of internet-capable technologies, the number of threats against cyber assets has increased immensely. As stated in the 2010 National Security Strategy, "The very technologies that empower us to lead and create also empower those who would disrupt and destroy."

"The very technologies that empower us to lead and create also empower those who would disrupt and destroy."

- *2010 National Security Strategy*

"Pentagon reveals 24,000 files stolen in cyber attack."

"Global cyber attack under way for 5 years"

Key cyberspace challenges

As the number of networked systems, devices and platforms continues to grow, cyberspace is becoming more deeply embedded in the critical infrastructure of our homes, businesses and nation. Given the increasing number and complexity of cyber threats, it is understandable that securing cyberspace dominates the agendas of business, community and government technology leadership.

The very technological innovations that enable our way of life have simultaneously made our cyber assets more difficult to protect.

Connectivity: As more and more data is migrated online, companies are expected to be more connected and open by allowing mobile, home computers and other internet-ready devices to access networks and services. While organizations are expected provide new internet capabilities to support a global economy, cyber actors are able to optimize their attacks across multiple platforms and devices. Effective cyber security requires innovative integration of technologies that keep pace with the rollout of new public-facing capabilities.

Evolution: The rate at which cyber threats evolve is of concern. Cyber adversaries are continually developing more sophisticated and dangerous capabilities that elude traditional cyber security measures. As more adversaries collaborate and combine resources, the level of innovation in cyber attack capabilities quickly outpaces the ability to adequately defend against them. Evolving cyber threat innovations are becoming smaller and more difficult to detect, yet have an equal or greater impact to cyber assets. Effective cyber defense requires an ability to evolve faster than our adversaries.

Speed: Cyber attacks are commonly considered fast - malicious hackers identify a target, and the attack is over

"The internet and e-commerce are keys to our economic competitiveness, but cyber criminals have cost companies and consumers hundreds of millions of dollars and valuable intellectual property."

- *2010 National Security Strategy*

almost as quickly as it began; however fast attacks are not the only concern. In 2010 more than 75,000 computer systems at nearly 2,500 companies around the world were hacked in one of the largest and most sophisticated cyber attacks to date. The attack not only shows the level of sophistication of the attackers. It also displays one of the greatest challenges to adequately securing cyber assets: the attack, discovered in January 2010, began in late 2008. Cyber attacks are not always quick. Some take time to unfold as computers are remotely controlled by the attackers, slowly infiltrating computers and networks until the end goal is achieved. Safely securing cyber assets requires an ability to detect malicious cyber activity over longer periods of time.

"Sophisticated cyber attack hits Energy Department's Pacific Northwest National Laboratory."

Big data: The amount of data generated each day about cyber assets is continually increasing at a staggering rate. Large enterprises generate terabytes of data each year related to network events, data downloads, running programs and various anomalies. Enabling effective cyber security protection requires an ability to quickly discern an acceptable event from a questionable one, identify its relationship to other events, and identify patterns that signify the occurrence of a cyber attack.

"Citigroup… the latest to fall victim to cyber crime…"

Decisioning: Proactive cyber security is based upon the quality of strategic and operational decisions that are made during critical times. And the quality of decisions is a direct reflection of the knowledge and understanding of past, present and future - understanding what happened, knowing what is happening, and proactively adjusting strategies and operations to protect against what could happen in the future. Individuals and organizations all make decisions using a process similar to the OODA Loop (Figure 1). With the growing potential of catastrophic cyber attacks, a cyber security OODA process must be measured in milliseconds, not seconds, minutes or hours. Effective cyber security requires automation of systems and decision-making processes. Decisioning must be fast and agile to keep pace with ever-evolving adversaries and operational conditions, and ensure the protection of cyber assets.

Resources: As with many IT leadership agendas, "doing more with less" has dominated the strategic landscape over the past few years. Current approaches to protecting against cyber threats puts demands on limited resources and can increase systems development and maintenance costs. Effective cyber security requires a robust framework of integrated technologies that minimize the strain on IT resources. The framework must be automated, scalable, performing, and be capable of empowering security experts to efficiently gather, analyze and make decisions about immense amounts of data.

Current approaches are not enough

To protect against cyber threats, enterprises have deployed a wide range of hardware and software defenses. Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS),

"Moreover, the speed of cyber attacks and the anonymity of cyberspace greatly favor the offense."

- *2010 Quadrennial Defense Review Report*

"Hong Kong trading halted by DDoS attack"

antivirus, firewalls and other network management solutions are strategically deployed to generate, identify and respond to events that meet the characteristics of malicious cyber activity. While these tools and technologies are sufficient to address part of the problem, they are not enough. As the sophistication of cyber attacks increases and the level of network exposure continues to outpace protection, these tools and technologies fail to adapt quickly enough to protect against savvy attackers. Unfortunately many IT leaders are continually overwhelmed by the challenges that these insufficiencies breed, and find themselves in a never-ending battle to fight cyber attackers from a reactive posture.

A cyber security framework

The OODA Loop (Figure 1) is a process for performing strategic and tactical decision-making. Developed by USAF Col. John Boyd (Ret.), OODA is based on an understanding that all organizations undergo a continuous cycle of interaction with their environment. The cycle is broken down into four overlapping processes: Observation: the collection of data; Orientation: the analysis and synthesis of data to form perspective; Decision: the determination of a course of action; and Action: the implementation of the decisions. Within the context of combat, the key to victory is to be able to create situations wherein one can make appropriate decisions quicker than one's opponent.

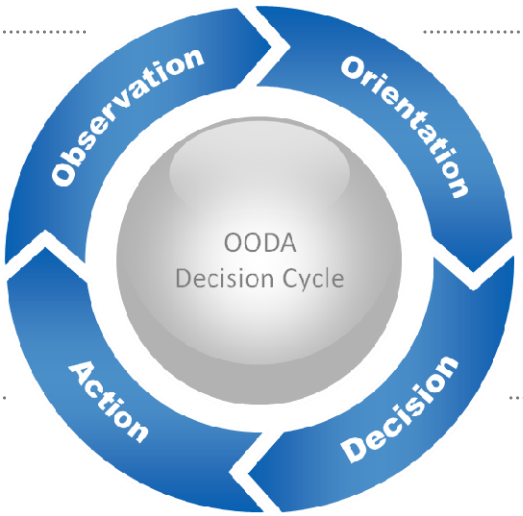
Figure 1: OODA Decision Loop

Observation

Capture, store, aggregate, filter and visualize event data from various sources throughout the infrastructure.

Orientation

Analyze captured data to identify patterns and event correlations that signify security holes or attacks in progress.



Action

Implement policies into operational systems to automate threat response or provide real-time decision support.

Decision

Execute "what-if" scenarios and analytic algorithms to find new strategies, policies and courses of action to mitigate threats.

"Every year, an amount of intellectual property larger than that contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and government departments and agencies."

- *Department of Defense Strategy for Operating in Cyberspace (July 2011)*

"Paris G20 files stolen in cyber attack."

"Emerging cyber threat: Advanced Evasion Techniques that combine to conquer."

Within the context of cyber security, organizations that can execute the OODA process quickly can gain an advantage over adversaries. When managed effectively, a foundational OODA process enables an organization to proactively close security gaps, assess potential risks and impacts, alter strategies and update operational systems with agility, consistency and precision.

By understanding the core purposes of each phase and how they relate to technological capabilities, the performance of each phase of the loop can be transformed and optimized to effectively protect against cyber threats. When integrated, the technological result is a framework capable of rapid evolution and response against cyber attackers characterized by persistence, coordination, purpose, sophistication and multilateral capabilities.

Observation: data collection

The first framework component enables capture and high-level correlation of event data. Multiple, dispersed sensors collect data from event sources across the enterprise. Real-time event correlation provides the first line of cyber defense by identifying event sequences, or lack thereof, that signify malicious behavior. Based on customizable policies, real-time events are streamed to automated decision engines for immediate resolution. As data are collected they are stored in operational data stores and warehouses to support the Orientation phase of the process.

Orientation: forming perspective

The second framework component combines data mining, analytics and visualization to enable deeper analysis of events. Predictive models leverage operational and historical data to determine the likelihood that a cyber attack is in progress. The models are designed to consider vast amounts of data, and are powerful enough to identify patterns that are too vast and complex for human identification. Predictive capabilities enable proactive closing of gaps that are being exploited, and provide foresight into other areas of risk in the cyber security grid.

Decision: course of action

The third framework component enables cyber security experts to assess risks and develop mitigation strategies using innovative decision optimization technologies. Decision models are developed to represent the current cyber security infrastructure in the physical domain. By utilizing captured event data and perspectives from predictive analytic assessments, cyber experts are able to simulate and model various attack scenarios using robust solvers to better evaluate cyber risks (Figure 2). "What if" capabilities facilitate prioritization of counter-measures, and create a better understanding of potential impacts to infrastructure and operational systems.

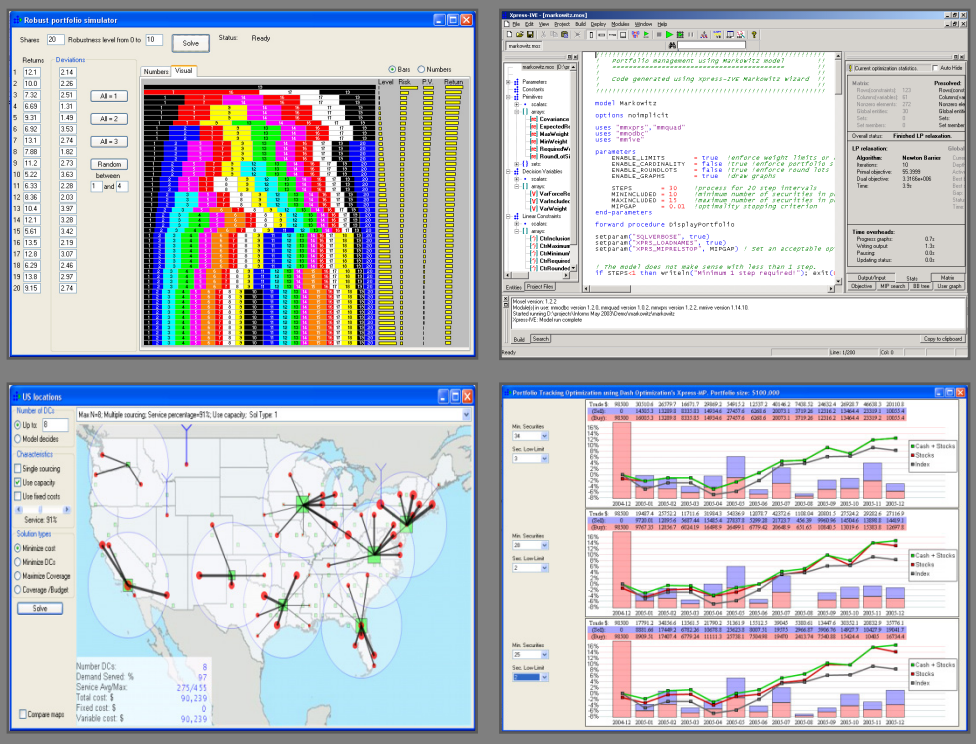
Action: implementation

The fourth framework component

Figure 2: Decisioning

By utilizing captured event data and perspectives from predictive analytic assessments, cyber experts are able to simulate and model various attack scenarios using robust solvers to better evaluate cyber risks.

"What if" capabilities facilitate prioritization of counter-measures, and create a better understanding of potential impacts to infrastructure and operational systems.



Screenshots courtesy of FICO (www.fico.com)

"Defending against these threats to our security, prosperity, and personal privacy requires networks that are secure, trustworthy, and resilient."

- *2010 National Security Strategy*

leverages real-time, operational decisioning capabilities to efficiently respond to operational conditions. Automated decisions are authored and exposed as application services that implement the policies, tactics and practices of the cyber security strategies. Responses are in the form of context-sensitive recommendations, or automated responses to re-route network traffic to compensate for outages or security compromises.

Visualization

A high-performing cyber security framework provides enhanced situational awareness through dynamic, interactive visualization of event data. Event capture, correlation and decisioning capabilities are integrated in a single interface to provide real-time perspective of ongoing cyber events throughout the enterprise (Figure 3). The visualization component of the framework is the core interface through which cyber experts perform tasks specific to each phase of the OODA loop. Cyber experts leverage a customizable front-panel display of visualizations including network diagrams, event severities and geographic maps to perform analyses, draw conclusions and make decisions about current and potential situations. Interface interactivity enables specialists to drill down into events to display relational information, run predictive models or launch optimizing solvers to determine plausible courses of action.

Access to real-time, meaningful and decision-oriented information enables

"Future adversaries will likely possess sophisticated capabilities designed to contest or deny command of the air, sea, space, and cyberspace domains."

- *2010 Quadrennial Defense Review Report*

experts to develop new policies for proactively reducing the existence and threat of cyber attacks. Where volumes of information exceed an ability to consume it and reason upon it, the innovative, integrated technologies synthesize deeper levels of meaning across data, further heightening situational awareness of the enterprise cyber domain. Where once sophisticated attacks could go unnoticed, a proactive cyber security framework ensures operational systems engage adversaries with fast, automated responses that close security gaps before significant damage is done.

Achieving high performance

Cyber security has traditionally been considered a technology problem. However high performing organizations are learning that to effectively fight and win the cyber war, cyber security must be an enterprise problem. By focusing on key tasks they are transforming their approach to cyber security, and developing proactive capabilities that reduce the potential for catastrophic cyber breaches.

Cyber Strategy

High performing organizations are weaving cyber security into their day-to-day business strategies. They are implementing technological frameworks that increase visibility into their cyber domain and protect their cyber assets from attack. In addition, they are actively educating their organizations, from C-level to programmers to assistants, on approaches to reduce internal cyber risks as well. Cyber strategy has become equally important as other enterprise

Figure 3: Visualization

Access to real-time, meaningful and decision-oriented information enables experts to develop new policies for proactively reducing the existence and threat of cyber attacks.

Screenshot courtesy of Edge Technologies, Inc. (www.edgeti.com)

"We will continue to invest in the cutting-edge research and development necessary for the innovation and discovery we need to meet these challenges."

- *2010 National Security Strategy*

initiatives such as CRM and SOA. Cyber strategy is becoming a planning and execution component of new business initiatives, product rollouts and partnerships. New positions are being created, including Chief Information Security Officers, further solidifying the dedication, and signaling the criticality, of protecting enterprise cyber assets from malicious adversaries.

Finding the gaps

High performing organizations are conducting war gaming sessions that simulate cyber attacks to uncover vulnerabilities and gaps in hardware and software security. Their findings lead to new strategies and capabilities that effectively close security gaps, and identify areas for improvement throughout the enterprise. Armed with this knowledge, organizations can begin the transformation to develop a proactive, lean-forward posture required to effectively combat cyber attackers.

Embrace innovation

Effective cyber security requires innovation. The sophistication of assaults and complexity of IT environments has increased beyond the capabilities of traditional tools and technologies. High performing organizations realize that addressing this challenge requires a reliance on resource, technological and organizational innovation. Technological innovation is at the forefront, and emerging tools, technologies and solutions are empowering organizations in the fight against cyber attackers like never before. High performing organizations are also heavily investing in acquiring and developing cyber expertise, capable of leveraging innovations to create agile, performing and scalable cyber defenses.

◊ ◊ ◊

Growing expectations for how organizations partner, interact with and share information with individuals and other organizations is continually pushing the envelope of cyber security. The number of cyber targets continues to grow, giving cyber attackers ample opportunity to disrupt, steal and destroy cyberspace assets.

The good news is that many organizations are already working to reach higher levels of cyber security performance. The same technologies that enable cyber attacks can also be used to defend our assets with equal effectiveness. Success requires organizations to invest in new strategies that empower users, systems and infrastructures, and technologically enable faster decision-making in the face dynamic operating environments.

Claye Greene, Managing Director of Technology Blue, is an IT strategist focusing on transformation and modernization initiatives. Contact us at info@technologyblue.com.

To learn more please visit
http://www.technologyblue.com/cybersecurity.htm

Technology Blue helps bring about meaningful change and lasting success through a broad range of outsourcing services covering:

- Strategy
- Application
- Infrastructure
- Management

Why partner with Technology Blue?

- Enhance core capabilities in key areas
- Leverage expertise to increase innovation
- Liberate resources to focus on core competencies
- Improve service quality
- Reduce costs
- Speed time to market
- Increase business performance
- Maximize profitability
- Solidify competitive advantage

A Technology Blue white paper

About Technology Blue

Technology Blue is an information technology strategy firm based in Pittsburgh, Pennsylvania.

With a strong commitment to deliver value through innovative approaches, tools and technologies, Technology Blue partners with its clients to help them transform and modernize to achieve higher performance.

Its home page is www.technologyblue.com.