Prepare. Protect. Prosper.

Cybersecurity White Paper

Maskelyne and Morse Code: New Century, Same Threat

In this issue:

- *The global cybersecurity threat as of Q2 2018*
- *U.S. Federal Government directives*
- *Preventive measures based on layered security*

Chameleon Integrated Services™

Executive Summary

The most compelling story in cybersecurity can be encapsulated in one word: overwhelming. A full-scale war is being waged, and in many cases against a small army of defenders deployed at internal business units. The cost of worldwide cybercrime is estimated to reach $6 trillion by the year 2021—a 200% increase from 2015. Further, cybercrime is described as the greatest threat to business, with cyberattacks increasing in size, sophistication, and damage—and they have become the fastest growing crime in the U.S.[1]

Where strong preventive and defensive cybersecurity operations should be in place for government agencies as well as for commercial and regulated industries—there is, instead, a growing gap.

The colliding problems of threat escalation, the cybersecurity labor crisis, and the poaching of qualified candidates into the arms of high-paying commercial employers has made the problem worse. This is happening while the pressing needs for cybersecurity solutions, staff, and IT modernization are growing exponentially.

We can't change the threat.
The cybersecurity threat will persist and evolve as perpetrators continue to improve their skills and expertise. We can mitigate the threat by changing the way we think about cybersecurity—the entire footprint—and then working systematically to put an effective incident response framework in place. The first step in the framework is *to establish a complete and thorough understanding of the network.*

Cyberwarfare Is the New Norm

Daily news that personal and sensitive information has once again been compromised is now routine, and can dangerously fade to background noise…for those who are unaffected *this time*. No person or business is immune to the risks of conducting transactions online. Engaging with others who communicate electronically, or who store data, generates risk automatically.

Data is high-value intellectual property that drives business and society—living at the heart of an individual's persona, a company's trade secrets, and an organization's ability to ensure continuity. And it has equally high value to those who will exploit it.

Information Attacks Predate World War I

It may be hard to imagine, but the world's first information assurance attack took place on a quiet June afternoon in 1903. About 115 years ago, John Ambrose Fleming was preparing to receive the first Morse code confidential wireless transmission sent by Guglielmo Marconi, with data traveling nearly 300 miles across the United Kingdom—from Cornwall to an exhibition in London (Marks, 2011).

"I can tune my instruments so that no other instrument that is not similarly tuned can tap my messages," Marconi bragged to the St. James Gazette in London earlier that year, claiming that messages could be sent privately over long distances, and only the intended recipient would be able to comprehend the electronic communication.

Meanwhile, around 1900, a talented engineer and practicing magician by the name of Nevil Maskelyne began sending wireless messages using Morse code during his performances to amaze, astound, and "read the minds" of his audience (Marks, 2011). What he was actually doing was communicating with his assistant in secret to accomplish and demonstrate his "mind reading" magic.

Maskelyne found himself at the mercy of Marconi's patents, and he wished to prove that Marconi (the future Nobel Prize winner) was blustering about the security of his wireless invention. To showcase the prowess of his knowledge and his own intellectual property, Maskelyne set up a small radio tower with the intention of intercepting Marconi's message and sabotaging the London exhibition by injecting a signal that sent his own set of transmissions to Fleming.

Maskelyne added a Morse code preamble to his demonstration, including repeating insults that called out Marconi and Fleming as "rats." He also skillfully added a smart but condescending limerick, complete with mocking verses using Shakespearean styles, to taunt and expose the audacity and hubris of Marconi and Fleming's claim of secret communications (Gascueña, 2016).

The Moral of the Story Is...

Marconi did not fully understand his network. He assumed that if he "hid" his messages well enough, no one would find him. Maskelyne took advantage of Marconi's confidence and executed an attack on core components of information security—exploiting vulnerabilities in the wireless transmission by sniffing out the frequency being used, which resulted in a compromise of confidentiality and data integrity.

If Maskelyne's attack had been triggered just minutes later, he might have compromised network availability—because the simultaneous transmissions would have likely become indecipherable from one another, and Marconi's message would not have been understood.

SitRep: The Enemy Isn't Going Away

Attackers always have a goal, ranging from financial gain to notoriety. An attacker's motives may not be immediately clear but can easily include activism, industrial sabotage, ego, or revenge as inspiration for their offensive. Even the least advanced bad actors are enacting their mission and working to realize their vision of success—although it may be as simple as using readily available tools and scripts in an attempt to compromise a school computer to change grades.

Understanding the threat model and the motivations of an attacker is key to examining all possible avenues of attack. Typically, attackers can be classified into one of three groups:

- *Advanced Attackers (Type I)*
- *Technically Savvy Attackers (Type II)*
- *"Script Kiddies" (Type III)*

Advanced attackers represent the greatest risk to a company's intellectual property or an individual's personal information. They work tirelessly to find new vulnerabilities and bypass security controls on interoperable systems. They have the advanced knowledge needed to create tools that automate their attacks, create efficiencies of scale, and generate code that exploits vulnerabilities. They work alone as highly skilled individuals or in groups of like-minded perpetrators, and sometimes they're even driven by nation states.

Advanced attacks are based on vectors aimed directly at vulnerabilities, including open-standards weak points at the intersections of commonality between systems. Weak points found are exploited by launching complex campaigns, delivering advanced-persistent-threat (APT) payloads, and betraying the basic trust of human nature through acts such as social engineering and phishing.

It's essential to understand that threat campaigns and APTs are based on an unfair, one-sided concept of time: *the attackers have time, whereas the defenders do not*.

Attackers can afford to be patient, but defenders must always be on and vigilant. This puts defenders in a persistent reactive stance, and adds to the challenge of keeping trusted networks trusted while preventing constant breach attempts against their systems. Having to continuously react, and not being able to effectively plan and act, can slow the process of converting from a legacy system to a modern system.

Legacy cybersecurity strategies—many still in place today—have been focused on building hardened walls as perimeters of defense. This approach often creates a bigger attack surface, results in more lost end points, and distracts valuable resources away from the high priority, high value assets (HVAs) that live further inside the perimeter, and require more security and protection.

Because the enemy isn't going away, and the cybersecurity defenses can't change the threat, an effective solution (discussed further in this paper) is to classify the HVAs as a high priority, and deploy a system of layered security.

Open Standards Can Create Open Doors

Our networks today are built on a foundation of open standards that were designed to create interoperability. They are necessary for the simple reason that data needs to transfer between disparate systems. However, the strengths and benefits of our interoperable systems can easily disguise and mask the risks that come with shared distribution.

As a method to ensure quality, efficiency, and security—and to defend against the inherent weaknesses of open standards networks—the Internet Engineering Task Force (IETF) and

the World Wide Web Consortium (W3C) work closely together to develop and promote standards for global systems that ensure interoperability.

Request for comments documents are issued by the IETF and W3C on proposed standards and then released with the agreed definitions and requirements that software and hardware designers, engineers, and developers strive to meet.

2018 U.S. Federal Government Guidelines

On the premise that open standards are a necessary building block for interoperable networks, we move to another foundational concept: modernizing, securing, and managing our networks. The U.S. Federal Government Guidelines present a well-engineered source of instructions, priorities, and requirements for government agencies, and they can work equally well when the principles are applied as guidance for private sector commercial and regulated industries.

In 2017, the comprehensive *Report to the President on Federal IT Modernization* was released with an outline, a vision, and recommendations for the federal government to build a more modern and secure architecture for federal IT systems.

First Recommendation Priority
Network modernization and consolidation comprises three points:

- *Prioritizing the modernization of high-risk HVAs*
- *Modernizing trusted internet connections (TIC) and national cybersecurity protection systems (NCPS) to enable cloud migration*
- *Consolidating network acquisitions and management*

Second Recommendation Priority
Shared services to enable network architectures comprises three points:

- *Commercial cloud services*
- *Accelerating the adoption and use of cloud email and collaboration tools*
- *Improving existing and additional security shared services*

Third Recommendation Priority
It is necessary also to provide federal network IT modernization resources. Agencies must be required to realign their resources appropriately using business-focused, data-driven analysis and technical evaluation.

These recommendations were incorporated into a subsequent document, the *2018 President's Management Agenda*—with IT modernization leading the agenda.

"Enhancing federal information systems to better serve the public is at the heart of the administration's IT Priorities"

The initiative includes three major goals:

- *Enhancing mission effectiveness*
- *Reducing cybersecurity risks to the federal mission*
- *Building a modern IT workforce*

The National Institute of Standards and Technology

In response to the cybersecurity landscape, threat vectors, and avenues of attack, the National Institute of Standards and Technology (NIST) has established guidelines for incident response that align with the President's 2018 directives on IT modernization, including the goals for improving critical infrastructure by partnering with private industry.

As an example of how NIST does its work—and how things can go wrong at the federal level—the failed incident response to the U.S. Department of the Interior (DOI) data breach (Reform, 2015) and subsequent failure on eight of nine systems to meet NIST minimum standards (Davis, 2016) showcase the urgent need to supplement native cybersecurity skill sets with expertise from private industry partners who are agile and responsive and can provide highly effective solutions.

Incident Response Framework

One of the most challenging sets of issues facing cybersecurity and network administrators is having a complete view of their assets:

- *How the data flows*
- *Where the critical information is processed and stored*
- *What the threat model looks like*

Marconi and Fleming had confidence, but they did not thoroughly understand the threat model for their new "secure" wireless communications method. Marconi underestimated his opponent. His hubris outweighed his planning, and the result was folly and damage to his public perception. Could he have put a better response framework in place? Could he have partnered with other experts, who may have added perspective or additional controls and systems that would have prevented or mitigated this attack?

It's common to find limited cybersecurity resources tasked with management of complex, compound networks. Often, the security teams work without a clear understanding of the networks, end points, HVAs, and resources because, over time, the networks have grown with added segments, or they have been adopted from reorganizations, mergers, and acquisitions—or they are simply the outcome of changes in administration or responsibility.

As a result, the typical cybersecurity organization is laser-focused on fixing current problems while constantly defending against the attacker. Scopes of work and task lists expand while at the same time there is a common hesitation to ask for help.

The NIST Incident Response Lifecycle (*NIST SP 800-61r2 Computer Security Incident Handling Guide*) is specifically intended to promote quality improvement and change management within cybersecurity organizations by assisting with plans and methods for the successful implementation of cybersecurity procedures and systems.

Corrective Action

Following on the NIST Incident Response Lifecycle and general corrective action, the federal government guidelines prioritize, and encourage, active engagement with private sector solution providers and subject matter experts. This approach is designed to produce successful, collaborative solutions that address and resolve root-cause problems in cybersecurity practices.

One successful private sector business model places the solution provider in the role of quarterback—serving as program manager/systems integrator, and leveraging partnerships with multiple vendors and software and hardware tool providers—to quickly bring a team of well-organized, skilled resources to bear.

An expert vendor team can operate in an efficient, fast-turnaround mode to plan and deliver results. A qualified team will bridge the gap between strategic vision and functional delivery by working closely with the client agency to create a situation analysis, problem definition, and corrective action implementation.

Delivery of results is typically in one of three formats:

- *Build and transfer to the agency or client*
- *Build, operate, and transfer to the agency or client*
- *Build and operate—vendor continues to operate and manage the solution*

Because the cybersecurity threat and IT modernization requirements are urgent, another key federal directive to its agencies is *go faster.* Cut through the red tape, change the way you think, rely more on outside vendors, make quicker buying decisions, and use readily available buying vehicles to optimize the purchasing process so the work can start sooner.

Three federal government buying vehicles help the work start sooner—and finish faster:

- *Technology Modernization Fund*
- *Other Transaction Authority (OTA)*
- *Sole Source—Direct Award—No Competition Required and Non-Protestable*

Layered Security with Deception and Detection

Layered security and deception technology are listed as two elements in the first group of key priorities defined in the federal IT modernization plan. They fall under the network modernization requirement to "modernize the TIC and NCPS programs," and they are specifically intended to support the requirements to identify and secure HVAs. The implementation method recommended in the layered security model is deception technology, which is more commonly known as deploying honeypots or honeynets.

Using Deception as Defense

Deception has been used in battle for thousands of years to lure the adversary into practices that either decrease their combat effectiveness or reveal their intentions and capabilities. The successful deployment of deceptive practices enhances the ability of the protagonist to adapt to fluid environments, effectively collect intelligence, and deploy resources.

A honeypot is an attractive resource on a computer network designed to entice attackers, improve defenses, and collect evidence for prosecution. By definition, a honeypot creates a trap where attackers unwittingly reveal themselves and their methodologies for gaining entry, elevating access privileges, creating transitive access to other systems, establishing backdoors to facilitate reentry, and covering their tracks. A honeynet takes this concept one step further and sets up intentional vulnerabilities to invite attack across a network.

Network deception technologies built on the honeypot/honeynet concept create an active engagement with the attacker on the cyber battlefield, and lure the attacker into an involuntary disclosure of their malicious intent to violate a system or network.

Although discussions began in the mid-1980's, the first publication describing a honeypot as part of a layered defense structure appeared in 1988 in the paper "Stalking the Wily Hacker" (Stoll, 1988) and was further popularized in his 1989 book, *The Cuckoo's Egg.*

In his book, Stoll recounts the tracking of a West German hacker and his attacks on the Lawrence Berkeley Laboratory, breaching computers operated by the U.S. military and its military defense contractors. By establishing a honeypot, Stole and his team were able to track the attacker and learn the tools, methods, and techniques being used.

Using Detection as Offense

From the attacker's point of view, the deployment of traps and decoys on a network creates an attractive opportunity for conquest and victory. Most of them want to beat the traps and decoys. The goal of detection is to entice the attacker—baiting for interaction with the detection tokens and triggering alarms.

Detection systems and tools are designed to reduce the number of false positive alerts. By sensing and calculating a combination of actions that occur against end points, the detection systems can limit themselves to high-probability alarms while collecting intelligence on the attackers and malware, even when zero-day exploits are used.

Well designed deception technologies create automated reactions to attacks, which can include the creation of additional tokens and the isolation of valuable resources. When deployed effectively, the deception approach enhances the more traditional heuristic detection and probability-based approaches to security.

Designing, installing, and deploying layered defenses requires expertise, along with an understanding of proactive defensive mechanisms and predictive analysis. The result is improved network integrity and the mitigation—or elimination—of risks associated with the exfiltration of data.

Summary: Change the Thinking on Cybersecurity

The need for cybersecurity is too often an afterthought, coming into focus only when the surprise and damage from an incident has occurred. The change of thinking needed is cultural. It's a conversion from reacting to problems to preventing problems.

Prevention is a basic premise of quality assurance with the objective to create "freedom from deficiencies in a product or process." Deficiencies make trouble for customers and providers—and in the cybersecurity arena they can have disastrous results.

Learning and understanding the cyber battlefield is of the utmost importance, and the sense of urgency cannot be overstated. A comprehensive approach to cybersecurity must be undertaken by organizations, and security must be natively built—from zero—into every element of the cybersecurity footprint, including every process, procedure, protocol, resource, individual, and the extended supply network.

A top-down approach that promotes full knowledge and understanding of the network, prioritization and identification of critical assets, data classification, and change management is essential to implement a truly holistic cyber defense that starts at the executive level and proceeds through every level of the organization.

Partnering with subject matter experts and vendors who have proven track records and can bring "the right tools for the job" is vital to success and will help to build a strong, modern IT structure and culture that will be able to defend and stand against highly aggressive, advanced, and unrelenting adversaries.

"Effective cyber defenses ideally prevent an incident from taking place. Any other approach is simply reactive."

— Sallie McDonald, Assistant Commissioner for the Office of Information Assurance and Critical Infrastructure Protection, Federal Technology Service and GSA

Although sponsored by the U.S. Government, these concepts, ideas, and principles can be applied as well to commercial and regulated industry—starting with the needs to change thinking, make cybersecurity a high priority, and thoroughly understand the network.

About Chameleon Integrated Services

With You from Strategic Vision to Functional Delivery

Helping you successfully capture transformational opportunities in IT modernization, cloud computing and building the workforce of the twenty-first century. Enhancing mission effectiveness by reducing cybersecurity risks. Chameleon is a proven and trusted solutions partner that delivers transformational results and successful outcomes to federal agencies, state and local governments, and commercial companies. Our unique approach is built around one set of goals—to help our clients: **Prepare. Protect. Prosper.**

We're an SBA-certified small disadvantaged business, minority owned enterprise, operating under the GSA 8(a) STARS II Governmentwide Acquisition Contract. Our headquarters are in St. Louis, Missouri, with offices in the National Capital Region; Belleville, Illinois; and Montgomery, Alabama.

Contact us

Chameleon Integrated Services

https://www.chameleonis.com
(314) 773-7200
inquiries@chameleonis.com

St. Louis Headquarters

3207 Washington Blvd.
St. Louis, MO 63103

Washington, D.C. Area Office

16701 Melford Blvd. Suite 131
Bowie, MD 20715

Endnotes and Bibliography

1. Morgan, Steve. (2017). "2017 Cybercrime Report." A 2017 report from Cybersecurity Ventures sponsored by Herjavec Group. https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf

Davis, J. S. (2016, August 12). "Interior Dept. must update access control standards to meet NIST guidelines - report." Retrieved from SC Magazine: https://www.scmagazine.com/interior-dept-must-update-access-control-standards-to-meet-nist-guidelines--report/article/529129/

Gascueña, D. (2016, June 01). *Nevil Maskelyne vs Marconi: a Hacker in 1903.* Retrieved from Open Mind: https://www.bbvaopenmind.com/en/nevil-maskelyne-vs-marconi-a-hacker-in-1903/

Marks, P. (2011, December 20). *Dot-dash-diss: The gentleman hacker's 1903 lulz.* Retrieved from New Scientist: https://www.newscientist.com/article/mg21228440-700-dot-dash-diss-the-gentleman-hackers-1903-lulz/

Reform, C. o. (2015, June 16). *OPM Data Breach - 6.16.15.* Retrieved from Department of the Interior: https://www.doi.gov/ocl/hearings/114/opmdatabreach_061615

Stoll, C. (1988, May). *STALKING THE WILY HACKER.* Retrieved from PDF Textfiles: http://pdf.textfiles.com/academics/wilyhacker.pdf

Authors: James R. McLaughlin, Brett R. Cox, Cheri R. McLaughlin, Jonathan J. McLaughlin