Prepare. Protect. Prosper.

Cybersecurity White Paper

Maskelyne and Morse Code: New Century, Same Threat

First in a series of cybersecurity white papers from Chameleon Integrated Services

In this issue:

- *The global cybersecurity threat as of 2019*
- *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: overwhelm. A full-scale war is being waged, and in many cases, against a small army of defenders deployed at internal business units. Cybercrime is predicted to cost the world more than $6 trillion annually by the year 2021, up from $3 trillion in 2015. Cyberattacks are increasing in size, sophistication, cost, and damage, making them the fastest growing crime in the U.S. and the greatest threat every company.[i]

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

While the pressing needs for cybersecurity solutions, staff, and IT modernization are growing exponentially, the colliding problems of threat escalation, the cybersecurity labor crisis, and the loss of qualified candidates to high-paying commercial employers have made the problem worse.

> "The overall tone of most security predictions for 2019 is not quite as treacherous as last year's forecasts, with very few apocalyptic cyberscenarios presented. Nevertheless, most experts still think the bad guys remain ahead of the good guys."
> -FireEye CEO Kevin Mandia

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, automatically creates risk.

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 Pre-Date 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. Over 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). In reality, he was secretly communicating with his assistant 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 a few 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.

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 offense. Even the least advanced bad actors are working toward their vision of success—which may simply be using readily available tools and scripts to compromise a school computer in an attempt 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 in 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. Whether it is a highly skilled individual, a group of like-minded

perpetrators, or an act driven by nation states, advanced attackers work tirelessly to find new vulnerabilities and bypass security controls on interoperable systems. Their advanced knowledge creates tools that automate the attacks, create efficiencies of scale, and generate code that exploits vulnerabilities.

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

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

Attackers can afford to be patient, but defenders must be vigilant. This creates an environment where defenders are in a persistent reactive stance. It further adds to the challenge of keeping trusted networks trusted, while preventing constant breach attempts against their systems. Having to continuously react, without 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—focus on building hardened walls as perimeters of defense. This approach often creates a bigger attack surface, results in more lost endpoints, 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.

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

Open Standards Can Create Open Doors

Networks today are built on a foundation of open standards, designed to create interoperability for the necessary data transfer between disparate systems. However, the strengths and benefits of interoperable systems can easily conceal the risks associated with shared distribution.

While open standards are a necessary building block for interoperable networks, they are also inherently weak and need to be defended. The Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C) work closely together to develop and promote standards for global systems. These standards help ensure quality, efficiency, and security of interoperability.

Request for Comments documents are issued by the IETF/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

Another important foundational concept is 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. These guidelines can also be successfully applied to private sector commercial and regulated industries.

> **"Enhancing Federal information systems to better serve the public is at the heart of the Administration IT Priorities"**

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, comprised of three points:

- Prioritizing the modernization of 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, comprised of 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
Provide federal network IT modernization resources.
Agencies are required to realign their resources appropriately using business-focused, data-driven analysis and technical evaluation.

The incorporation of these *Federal IT Modernization* recommendations leads the agenda for the *2018 President's Management Agenda*.

The initiative includes three major goals:

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

National Institute of Standards (NIST)

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

A failed incident response to the U.S. Department of the Interior (DOI) data breach is an example of how NIST works, and how things can go wrong at the federal level (Reform, 2015). After the breach, it was discovered that 8 of 9 systems failed to meet NIST minimum standards (Davis, 2016). This showcases the urgent need to supplement native cybersecurity skill sets with expertise from private industry partners who are agile, responsive, and provide effective solutions.

Incident Response Framework

A complete view of assets is a major challenge for cybersecurity and network administrators. They must consider:

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

Marconi and Fleming had confidence but did not thoroughly understand the threat model for their new "secure" wireless communications method. Marconi underestimated his opponent and allowed his hubris to outweigh his planning. 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 for additional perspective or advice on controls and systems that may have prevented or mitigated the attack?

It is common to find limited cybersecurity resources tasked with management of complex compound networks. Because networks evolve over time, the security teams often work without a clear understanding of the network endpoints, HVA's, and resources. Networks grow with added segments, are adopted from reorganizations, mergers, acquisitions, or are simply affected from 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, yet many are reluctant 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 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/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, a key federal directive is to *go faster*. Cut through the red tape, change the way you think, rely more on outside vendors, make quick 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 technologies are listed in the first group of key priorities in the *Federal IT Modernization* plan. They fall under the network modernization requirements to "modernize the TIC and NCPS programs" and 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 that is designed to entice attackers, improve defenses, and collect evidence for prosecution. 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 re-entry, 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 creates an active engagement with the attacker on the cyber battlefield and lures the attacker into an involuntarily disclosure of their malicious intent to violate a system or network.

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

In his book, Stoll recounts the tracking of a West German hacker who attacked the Lawrence Berkeley Laboratory, breaching computers operated by the U.S. military and its military defense contractors. Stoll and his team established a honeypot to track the attacker and learn the tools, methods, and techniques being used.

Using Detection As Offense

From the attacker's point of view, network traps and decoys present an attractive opportunity for conquest—a challenge that must be beat. Detection entices the attacker by baiting for interaction with the detection tokens and trigger 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 endpoints, 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 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

Cybersecurity is all too often an afterthought, coming into focus only after the surprise and damage has occurred. A cultural change in our thinking is necessary to convert the approach from reaction to prevention. 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, which can produce disastrous results in the cybersecurity arena.

Learning and understanding the cyber battlefield is of the utmost importance, and the sense of urgency cannot be overstated. Organizations must take a comprehensive approach to

cybersecurity. Security must be built 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 proven vendors that will bring the right experience and tools, is vital to success. The right partnership can build a strong, modern IT structure and culture that will defend against highly aggressive, advanced, and unrelenting adversaries.

Although sponsored by the U.S. Federal Government, these concepts, ideas, and principles are applicable to commercial and regulated industry—starting with the need to change thinking, make cybersecurity a high priority, and produce a complete understanding of the network.

> **"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 General Services Administration*

About

Chameleon Integrated Services provides agile IT integration services that bridge the gap between strategic vision and functional delivery. Our passion is to enable our clients to: Prepare. Protect. Prosper.

We're an SBA certified small disadvantaged business headquartered in St. Louis, Missouri with satellite offices in Washington, DC, Montgomery, AL, Denver, CO and Salt Lake City, UT. We bring a nimble business structure marked by fast-response, comprehensive solutions, and an across-the-board commitment to quality, innovation, and integrity.

Contact us

Chameleon Integrated Services

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

Endnotes

[i] https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

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