



SENIOR LEADER PERSPECTIVE: DANNY MCPHERSON, VERISIGN

Danny McPherson is Chief Security Officer for Verisign where he is responsible for strategic direction, research and innovation in infrastructure, and information security. He currently serves on the Internet Architecture Board (IAB), ICANN's Security and Stability Advisory Council, the FCC's Communications Security, Reliability, and Interoperability Council (CSRIC) and several other industry forums. He has been active within the Internet operations, security, research, and standards communities for nearly 20 years, and has authored a number of books and other publications related to these topics. Previously, he was CSO of Arbor Networks, and prior to that held technical leadership positions with Amber Networks, Qwest Communications, Genuity, MCI Communications, and the US Army Signal Corps.

NSCI: What do you see as the key(s) to improving the security of our nation's critical infrastructure?

MCPHERSON: A good starting point is recognition that out of the gate there is an existing and expanding set of vulnerabilities and exploits that can be used to compromise critical infrastructure without the need for physical access. Couple the fact that more critical infrastructure is being instrumented via networked systems than ever before with the wide-scale deployment of well-known operating systems, protocol stacks, programming libraries, and implementations, running on widely available commercial or commodity hardware within that infrastructure, and you quickly realize that critical infrastructure is commonly at least as vulnerable as your average Internet-connected system. Assuming rigid perimeters or closed networks are secure in this day and age, irrespective of the application, is pure lunacy. 'Air gaps', obfuscation and perimeter-based defenses alone are clearly insufficient, particularly when people are involved, and certainly against persistent and motivated attackers.

Once you've met compliance objectives that set a baseline and largely solve yesterday's threats, a good next step is to assume your perimeter has been breached, and determine how you detect, contain, and minimize your exposure if and when that occurs. Those involved with network security need to fully understand the content and transaction-level intricacies of the systems which they operate, to profile how those systems behave during steady state conditions, and possess the capability to detect when those systems deviate from expected behavior; e.g., who, what, when, where, how and why those systems communicate with other systems. In general, this lends itself to a systemic approach to network security, as it requires full enumeration and express consideration of the entire attack surface, with particular care given to overlay systems and interdependencies between those systems. From there, putting more preventative controls in place is more plausible.

NSCI: Some have stated their belief we are going too fast with implementation of the "smart grid" while assuming we can fix security later, as happens with many initiatives. What do you think?

MCPHERSON: I think that's very risky! Security needs to be indigenous, inherent and expressly baked into the architecture, not bolted on after the fact. The underlying problem here is that with non-security minded folks it typically only matters - or is given due consideration - *when it matters*. That is,



Keeping Cyberspace Professionals Informed

security is commonly compromised during specification or build time as a result of perceived excessive cost or ease of use; and then it's reassessed after some aspect or element is exploited. With critical infrastructure today there's no excuse, you simply can't compromise on security, as the results can be catastrophic.

NSCI: What are a few of the most common shortfalls you see with an organization's cyber incident response plan?

MCPHERSON: The most common shortfall is that many organizations lack a well-defined incident response team, even if derived from overlay resources. If you don't have an incident response team odds are pretty good that you don't have a plan - even an insufficient one. If you don't have a plan then you haven't been testing and refining it periodically with penetration tests, table tops, and other exercises. If you haven't exercised your plan then you haven't considered what aspects of it, or various tools and controls you have in place, are insufficient and need to be adapted. Most of the work with incident response planning is the preparation phase, incident response itself should be well defined and largely mechanical relative to the assets and devices that were impacted.

If I had to put my finger on a few particular common issues: lack of asset (physical and information) classification driving response handling; lack of access to critical out of band information such as communications and support details (e.g., internal escalation contacts, network service providers, vendors, law enforcement, etc.) in the face of system availability issues (e.g., you can't access the plan because it's on a server you can't reach); lack of established baselines and what constitutes steady state, thereby allowing anomalies and malicious activities to be detected; and finally, lack of an explicit post-mortem phase that forces feedback about what worked and what didn't. That said, as even Mike Tyson knows, "Everybody's got a plan - Until they get hit!"

NSCI: The Department of Defense recently conducted a pilot project that included sharing threat information with the private sector. What are your thoughts on this initiative and some possible next steps that are still needed?

MCPHERSON: The ability for private sector to consume and act on DoD threat indicators is paramount to protecting national infrastructure. However, a facility for information to be shared in context such that corporations can consider the full extent of their exposures and consult with legal or other entities in the organization as appropriate needs to exist, just as with any other incident. In general, broader engagement and a well-defined information sharing infrastructure that's multi-party and enables bidirectional communications and real-time information sharing is key to enabling both reactive and proactive controls.

NSCI: What do you see as a few of the cybersecurity areas where additional research is needed and should be a priority?

MCPHERSON: Research and development in the areas of verifiable trusted platform and application implementations, network access control solutions and auditable user-centric network transactions is



critical (i.e., realizing the full expanse of the who, what, when, where, how and why above, and coupling into the future with more preventative controls and explicit security models). Enumerating and minimizing system interdependencies and transitive trust models is also critical, as is evolving from inherently reactive and beleaguered blacklisting solutions - such as traditional anti-virus and IDS systems - to more refined and explicit security controls.

NSCI: What should we be doing to ensure cybersecurity research is better coordinated and shared between government, industry, and academia?

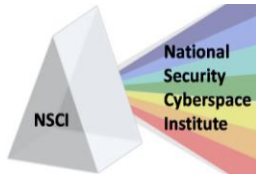
MCPHERSON: The key here is that we collectively make an express attempt to refine strategies and associated tactics. If explicit actions to establish frameworks, systems, facilities, and sustainable funding and incentive models are not taken, it's simply not going to resolve itself. Likewise, we're not going to cultivate the next generation of security-minded research and development folks or have the capability to innovate and benefit from the intelligence of the aggregate. Most anyone in the cybersecurity arena today surely realizes the pain threshold has long ago eclipsed the perceived expense of being more proactive in our approach. We're already at that point where we need to bake it in after the fact, and ensure that security is top of mind and indigenous into the future.

NSCI: There has been a lot of debate regarding the balance and trade-offs between personal privacy and a more secure Internet. What are your thoughts?

MCPHERSON: I'm sympathetic to the privacy concerns raised and consider the tussle between security and privacy to be a predominant consideration in today's cybersecurity landscape. However, without actor attribution and prosecution you can't establish deterrent controls that curtail malice online, period. And if you can't lessen that malice, the trust and reliance and innovation that have brought billions to a single global Internet will continue to erode, potentially driving balkanization or other negative effects. Striking the right balance between security and privacy is critical.

NSCI: Many have the opinion that the internet is inherently insecure since we are now using for many things it was not designed for. What are your thoughts on starting over with one internet that is more open and another that is more secure?

MCPHERSON: If we were to hit the reset button I'm certain we wouldn't end up with an Internet that's more open than the one we know today. Many of the primitives that have made the Internet successful, from packet-switched statistical multiplexing accommodating inherent multi-tenancy, and IP's layered modular protocol architecture, to an inherent "any to any" connectivity platform, employing the "End to End" principle that enables the edges to adapt and innovate with very little impact to the network - the very fact that the Internet has been used for so many things that it was not designed for is a testament to it's success! All that said, there are lots of incremental things we could do to better secure today's Internet, from network level authentication and integrity mechanisms, to secure inter-domain routing and registration systems, we just need to find the incentive models that can make this a reality and the ability to adapt while in flight without compromising the availability or integrity of the infrastructure in the process. Intermediate or longer term, the ability to consider new network layer



Keeping Cyberspace Professionals Informed

addressing architectures that adapt more effectively to mobile, multi-homed, and multi-protocol end systems and devices, and allow the network locator and end system identifiers to be decoupled (unlike IPv4 and IPv6), would allow stable end-to-end network layer identifiers for devices, upon which various business logic can be applied. From a purist perspective, removing all the middleboxes in the network that exist today and are complicating “end to end” - and are increasing in the face of IPv4 and IPv6 transitional co-existence - would be gravy!

NSCI: Many have talked about a potential "Cyber Pearl Harbor," specifically as it relates to a major cyber attack on our critical infrastructure. How real would you say this kind of threat is?

MCPHERSON: There are lots of attack vectors that could have wide-scale effects, direct, kinetic and collateral in nature. We've seen many empirical examples of these as a result of both unintentional and malicious actions. In general, we're doing a better job of accessing and increasing the resiliency of our critical infrastructure, but we've got an uphill battle.

NSCI: Is there anything else you'd like to add?

MCPHERSON: My father-in-law always told me “locks only keep honest people out!” While he shared this in a different context, it's extremely applicable in today's cybersecurity landscape. With determined and persistent attackers and constantly expanding networked resources, malicious actors only need to be right once; we have to be right all the time. We need to continue to recognize and invest proactively, evolving controls in order to proactively mitigate the threat du jour, as well as to anticipate the threats of tomorrow. Furthermore, establishing information sharing frameworks and foundational elements in education, research, and development that will best enable the next generation of cyberspace professionals for the mission ahead is critical.

NSCI: Thank you very much for taking the time to visit with us.