nemertes RESEARCH
Independence. Integrity. Insight.

2017

All Together Now: Securing the Internet of Things

IoT is key to many Digital Transformation projects—is your network ready?

Internet of Things pushes myriad new endpoints onto the network, but security for IoT is still in its early days. IT needs a network that can supporting as many devices as the business needs, wherever it needs them, while actively participating in securing the whole environment.

Compass Direction Points:

- **Companies successful in Digital Transformation use IoT more than others.** Leaders in Digital Transformation use IoT 31% more often.
- **Most companies spending more on security in 2017, with analytics as a focus.** Nearly 80% of companies are spending more on security in 2017, with an average increase of 42%, and analytics and threat detection are the top spending targets.
- **Visibility and security need to be everywhere.** IoT devices can be anywhere in the network, and may move; campus and branch networks have to help secure this complexity.

By John E. Burke
Principal Research Analyst and CIO
Nemertes Research

Table of Contents

Table of Figures

Executive Summary

The Internet of things is at the center of many organizations' digital transformation strategies, but often without consideration of the fact that security for IoT is in its infancy. As organizations rush ahead, intent on realizing the business value of IoT, addressing security gets left to the last minute--even *after* a system is in production. This risk/reward trade-off is insupportable when applied to many of the critical systems using IoT: industrial controls, energy infrastructure, transportation, and water, power, and gas distribution networks.

Unfortunately, as we have seen in recent, highly publicized Internet attacks, inadequately secured IoT not only jeopardizes the IoT devices themselves, it also provides both a dangerous infection vector for more conventional systems, and a potent tool for attacking the entire enterprise. IoT devices can all serve as host to self-propagating worms whose ultimate target is laptops or servers. Likewise, any device active on the network can, if compromised, attack either an organization's information infrastructure or its operational technology infrastructure.

The solution? Businesses and utilities need to take a security-first approach to IoT implementations. This involves embedding both *visibility* and *protection* into the IoT networks. Deeper visibility into IoT devices' network utilization and behavior improves both network management and network security. More effective protection—more active and dynamic use of edge network devices to implement security policies—has two main benefits. By moving enforcement closer to the problem, it increases security responsiveness; and it can also take some of the load off centralized solutions.

To start moving toward more secure IoT, IT professionals should:

- Evaluate all IoT efforts under way or currently proposed
- Evaluate the network's ability to supplement the security of IoT solutions
- Implement device security plans where feasible
- Evaluate new network solutions to meet requirements the existing network can't meet
- Collaborate with facilities teams on the infusion of intelligence into the systems they manage, to ensure proper security and network management
- Enlist the business lines with IoT initiatives under way in building a business case for acquiring whatever is needed to secure IoT properly

The Issue: Digital Transformation Loves Internet of Things, but Security is an Afterthought

The Internet of Things (IoT) is at the center of many organizations' Digital Transformation strategies—half of the most successful companies are putting more money than their less successful peers into IoT (please see Figure 1). They often do so, though, without consideration of the fact that IoT security is in its infancy. There are no broadly accepted security technology standards for IoT, neither unique to it nor IoT-specific variations on technologies applied elsewhere in the environment. Nor are there broadly accepted and implemented standard IoT security practices.

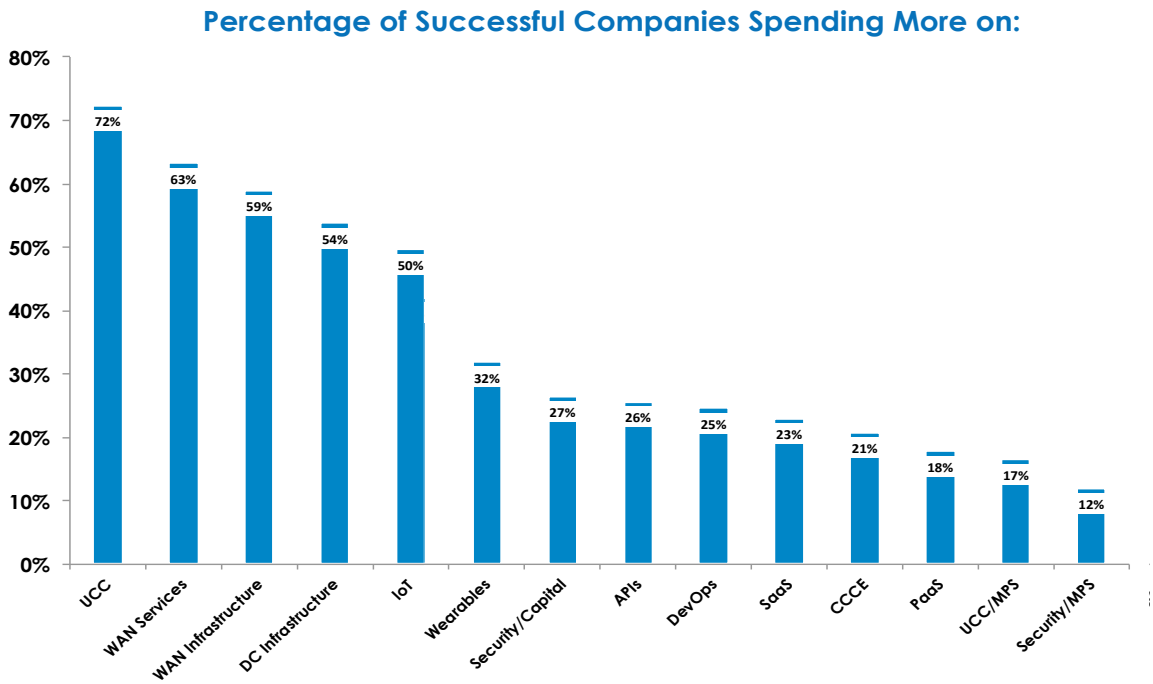

Figure 1: Successful Digital Transformation companies out-invest others on IoT more than on Security

Yet most organizations lack IoT-specific security policies, frameworks, and best practices—leaving them on their own in deciding what to do and how to accomplish it. They know they should extend some standard technologies and practices—encryption and authentication, access control and separation of duties—but which, when, and how?

In light of this lack of guidance, organizations intent on realizing the business value of IoT push ahead, and (as so many times before) postpone decision and action on security, willing to sweat those details at the last minute—or even after a system is in production. Few put IoT among their top security concerns. (Please see Figure 2.)

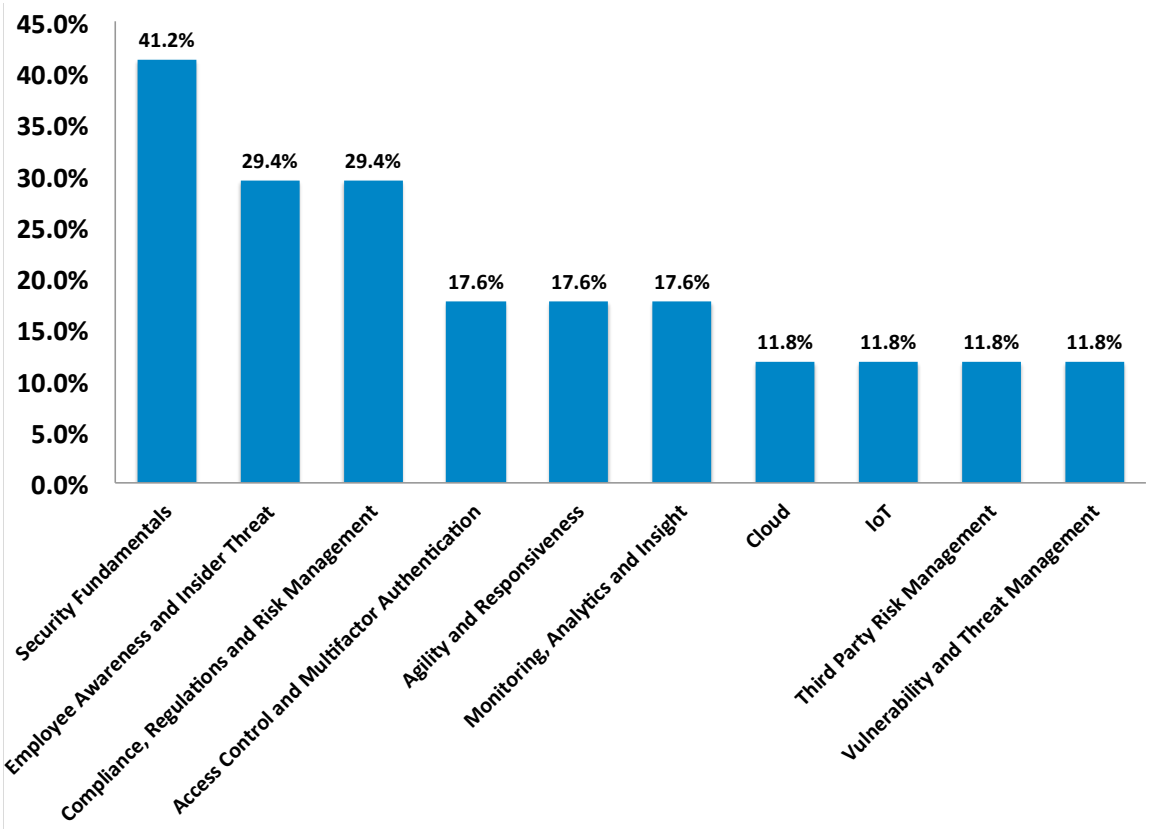

Figure 2: Fewer than 12% of companies list IoT among their top security concerns

This kind of cavalier, headlong plunge sans proper security is obviously insupportable when applied to many of the other kinds of systems falling under the aegis of IoT:

- manufacturing systems such as industrial robots and petroleum refinery controls
- power plant controls
- water, power, and gas distribution networks
- building environmental controls
- automobiles
- traffic control systems

The Challenge: Cyberspace Interacts With Reality

The important thing to understand with IoT systems such as these is that they incorporate bi-directional interaction with reality. That is, they not only provide information back to the enterprise (as do various types of sensor networks); they also affect the physical environment directly. Such networks are sometimes referred to as operational technology IoT networks.

As far back as 2010, with the Stuxnet attack on Iranian nuclear reactors, hackers demonstrated the ability to affect the actual physical operation of systems via cyberwarfare. Security professionals may recall that Stuxnet infected specific SCADA systems manufactured by Siemens. In particular, the virus installed code into the programmable logic controllers that modified the frequency of operation, thus changing the rotational speed of the motors.

Stuxnet may have been the first, but by no means will it be the last. While the 2015 zero-day exploit by white-hat hackers Charlie Miller and Chris Valasek on the moving Jeep Cherokee was for demonstration purposes only, it represented a proof-of-concept: attacks on these types of industrial systems can take down energy systems, crash cars, and wreak widespread havoc in the physical world.

Yet many, if not most, organizations roll out this mission-critical industrial and operational technology infrastructure on the same general-purpose security platforms as they do their enterprise business applications. Often these general-purpose security platforms are sub-par to begin with; they can't adequately protect a company's email, let alone its industrial control systems. The solution lies in taking a security-first approach, and embedding security throughout the network, both to enable real-time monitoring, and to provide defense and protection.

Too Many Types of Vulnerable Nodes

To see why this approach is necessary, it's important to look at the different ways that an IoT network can affect an enterprise. Specifically, IoT devices can provide both a dangerous vector of infection for more conventional systems, and a platform with which to attack other targets.

Infection: IoT as Vector

In coming years, IoT devices will be everywhere in the network, as more and more kinds of intelligent device come on line. Smart televisions, IP telephones, conferencing systems, and IP security cameras are widely deployed already. Newer generations of device such as intelligent thermostats and environmental sensors are spreading rapidly.

Whatever the impact of the compromise of one (or all) such devices in an environment on the services they deliver, it can pale in comparison to the risk created for the rest of the environment. That's because many of these intelligent, embedded, and networked systems—which are, after all, often just tiny Windows or Linux computers running specialized software—can serve as host to self-propagating worms whose ultimate target is the more conventional laptops or servers in the environment. The television or DVR is just a reservoir from which an

infection can reach its true targets, and the more broadly such potential reservoirs are distributed through the environment, the more risk to those targeted platforms.

Attack: IoT as Weapon

A more serious risk is that IoT devices can not only spread infections, but serve as a weapon directly. That can include affecting a company's information infrastructure by crashing systems and implementing denial-of-service attacks---but as noted above, IoT networks can crash cars, shut down energy generation plants and distribution systems, and take down manufacturing plants and other operational technology infrastructure. Targets will almost certainly include industrial controls and medical devices.

SCADA systems. The U.S. Department of Homeland Security recently issued a report stating that SCADA attacks are steadily increasing, with 295 incidents tracked in 2015, the latest year for which figures are available. It's almost certain that these numbers will skyrocket in 2017.

Industrial control systems (ICS). ICS-CERT, the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team has documented multiple attacks in recent years, and predicts these will increase.

Health-care machines and systems. In early 2017, Abbott Labs issued updates to its St. Jude artificial hearts, several months after the U.S. government launched a probe into claims they were vulnerable to potentially life-threatening hacks.

Overlooked IoT: When Traditional Devices Go Rogue

Formal IoT initiatives aren't the only challenge. An even greater—yet often overlooked—challenge is when devices in traditional networks (HVAC, lighting, etc) are upgraded and in the process acquire newly embedded intelligence. Many HVAC systems, for example, now come with embedded controllers, putting a new and vulnerable IT system where there was none before. As with more formal IoT networks, often manufacturers insert this intelligence without being aware of the security implications—including the need for regular upgrades, support, bug fixes, and security hardening.

Yet IT is often entirely unaware of these newly enhanced networks, for the very good reason that IT is typically out of the loop when it comes to facilities. Only about a third of IT security organizations have oversight over facilities security (please see Figure 3), so odds are most IT groups won't know when newly intelligent and vulnerable systems comes on line. And even where there is some formal relationship with facilities already, it can be focused so closely on traditional

facilities security (such as door locks and security cameras) that previously peripheral concerns such as air conditioning systems get overlooked.

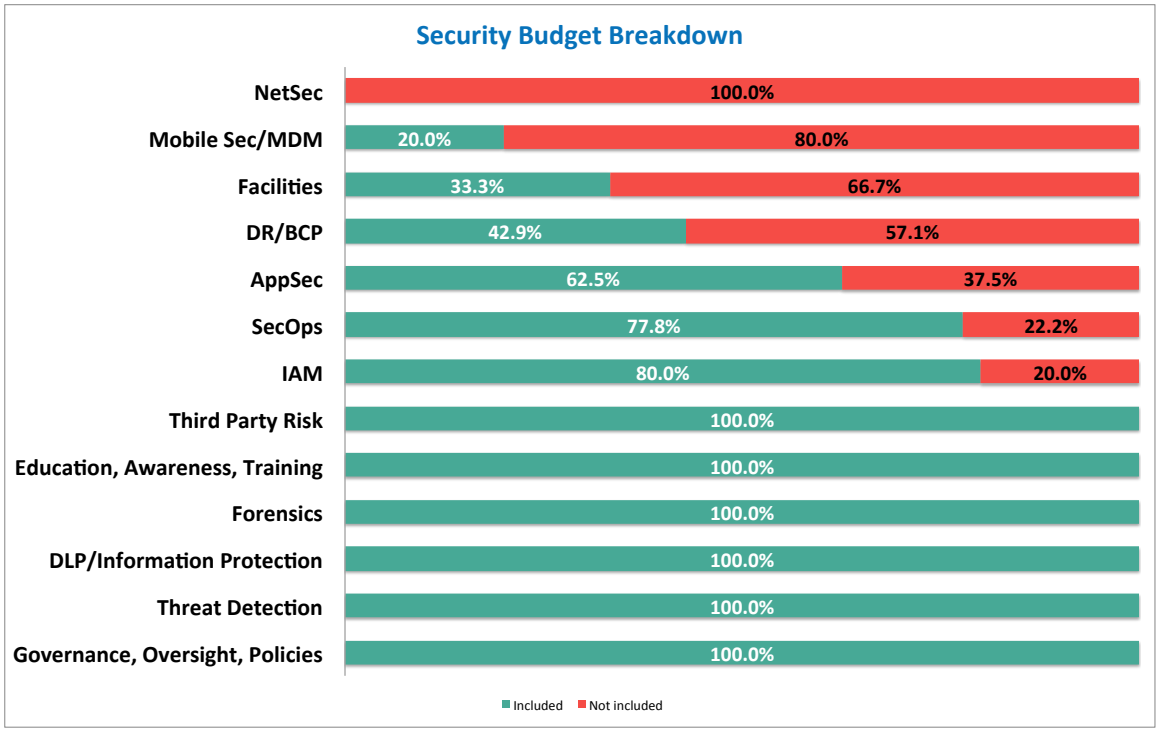

Figure 3: Two-thirds of security departments have no budget for or oversight on facilities efforts

To fix this, security staff will have to engage regularly with facilities departments to review planned changes to the environment and apply appropriate network security measures. This will stretch already overloaded security staff even further, of course, increasing pressure to broaden and deepen use of security automation, as well as professional or managed services. IT will also have to consider increasing security staffing, possibly explicitly in conjunction with facilities and preferably funded partially out of that budget.

The Solution: Immune Boosters

Businesses need to look to their networks not just to connect IoT devices but to help secure their use. The network can make up for shortcomings in the devices and platforms themselves; or, where it is present, work in collaboration with their native security functionality.

Businesses have their sights set on the right technologies in their security budgeting plans: analytics, threat intelligence, security monitoring, and endpoint security. (Please see Figure 4.) Security and network staff just have to make sure they are considering IoT's needs and characteristics as they define requirements for

solutions in all these spaces. They must then keep a focus on IoT in their thinking as they incorporate these solutions into their architectures and implement secure networks for their evolving environments.

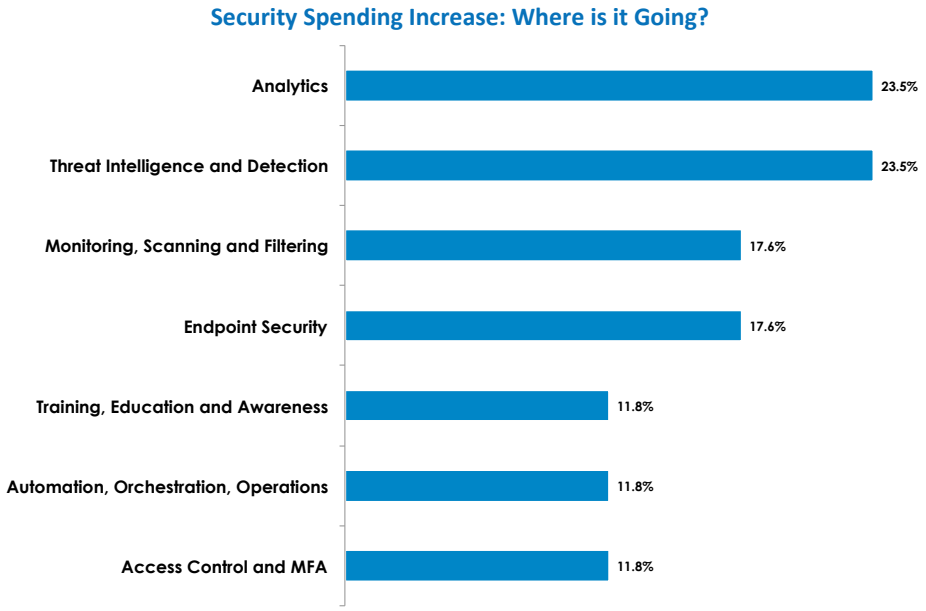

Figure 4: Seventy nine percent of businesses increasing security spend in 2017...with analytics leading the way

Step One: The All-Seeing Network

The network can help IoT security first by providing broader and deeper visibility into network utilization by IoT gear. It can provide insight into every device's behavior. Granular and historical monitoring data will allow analytics tools, whether built into the network or simply drawing data from it, to establish a baseline for normal activity and thereafter to spot anomalies and, among the anomalies, threats.

To do the best job of understanding normal traffic flows—and therefore of spotting threatening variations from the norm—analytics solutions need data from every level and segment of the network; from edge to edge. The only ways to provide this kind of visibility are to establish a parallel data collection network to provide data to an analytics solution; or to build analytics into the production network. Creating a shadow network attached to the production network at every switch but used solely for management and monitoring is both complex and expensive. A network that can take up the burden of analysis, in whole or in part, is simpler to design, deploy, and maintain, and able to spot and respond to issues more quickly.

Step Two: The All-Protecting Network

It is not enough to see problems, though. The whole network must also help defend the enterprise.

Pervasive protection through use of the entire network to enforce security policies will improve security in several ways: it will speed detection, shorten response times, and simplify propagation and enforcement of any resulting changes to policy.

Pushing more detection and enforcement out toward the edge of the network will decrease the workload on centrally located security appliances. When edge and aggregation switches do more traffic filtering, central firewalls will have less traffic to process. IT will be able to scale them down some, which can drive a significant savings.

Consider the case of a multi-pronged attack focused on compromising a client account database. It includes a direct, application level attack that relies on exploiting a buffer overflow created by a parallel, volume-based denial of service attack. The denial of service attack is launched via IoT, courtesy of hundreds of infected video cameras in every one of a hundred branches.

An intelligent and actively secure network would spot the anomalous traffic flows being aimed at the database server by the security cameras. It could also respond immediately, and stop the traffic where it first hits the network instead of relying on (and possibly overwhelming) routers or firewalls between the various branch and HQ networks and the data center. Moreover, stopping the attacks right where they enter the network stops an ancillary denial of service attack on the WAN itself that the compromised IoT nodes would create as a side effect of trying to swamp the database service.

Conclusion and Recommendations

The Internet of Things will be at the center of many organizations' digital transformation strategies. The time has come for them to realize that they cannot push ahead with IoT without facing head on the need to secure it, even when the IoT initiative itself seems low risk. Inadequately secured IoT jeopardizes the whole organization, as both a vector of infection for more conventional systems, and as potent tool for attack.

Businesses need their networks to pick up more of the burden of security, to help detect and protect against both current and emerging threats. The all-seeing and all-protecting network will build on whatever IoT solutions can do for self-protection and make up for whatever they lack. Deeper visibility into IoT devices' network utilization and behavior will improve cybersecurity. More active, dynamic use of the

whole network to implement security policies will both move enforcement closer to the problem and improve the effectiveness and efficiency of centralized solutions.

To start moving toward more secure IoT, IT professionals should

- Identify and assess all IoT efforts under way or currently proposed; this includes working with facilities teams to find "stealth IoT" deployments resulting from the infusion of intelligence and network connectivity into solutions that previously lacked them
- Evaluate the network's ability to provide deep visibility into and understanding of IoT device behaviors
- Evaluate the network's ability to supplement, all the way to the edge, the security of IoT solutions
- Identify new network solutions to meet requirements the existing network cannot
- Enlist business lines with IoT initiatives under way as well as facilities teams in building a business case for acquiring whatever is needed to secure IoT properly.