WEBINAR SUMMARY

January 21, 2020

IndustryWeek

Securing the Edge: Cybersecurity in the Age of IoT

Larry Ponemon, Ph.D., Chairman and Founder, Ponemon Institute

KEY TAKEAWAYS

- Lack of visibility into systems plays a key role in IT security gaps.
- IoT is widening the gap, straining standard and conventional security approaches.
- Organizations see the third-party IoT risk, but are behind in managing it.
- Start laying the right foundation now to manage the growing IoT cybersecurity challenge.

in partnership with

AVNET

OVERVIEW

Security teams today are overwhelmed with the number of new productivity, profitability, and customer experience initiatives they are expected to support. Mobility, bring your own device (BYOD), cloud, and Internet of Things (IoT) are all becoming vital to daily business operations, but at the same time, they create new security risks.

IoT, in particular, widens IT security gaps, opening new vectors for cyber attacks and data breaches. As businesses work with third-party IoT devices and applications to monitor and collect data, they expose the organization to even more risk. When implementing IoT solutions, organizations need to be fully aware of the many risks and plan for closing existing and new security gaps as quickly and efficiently as possible.

CONTEXT

Dr. Larry Ponemon shared findings from two studies focusing on IoT risks: 1) the Ponemon Group's *Closing the IT Security Gap with Automation: AI in the Era of IoT* and; 2) the Santa Fe Group's Shared Assessments *Third Party IoT Risk Study*.

He used these studies to frame some of the key challenges facing organizations today, as well as high-level steps security teams can take to close security gaps.

KEY TAKEAWAYS

Lack of visibility into systems plays a key role in IT security gaps.

Coupled with a lack of visibility and control, organizations are facing numerous and growing security gaps, which diminish a company's ability to detect, contain, and resolve security incidents. As IoT systems expand, organizations are also seeing growing security gaps in their system infrastructures.

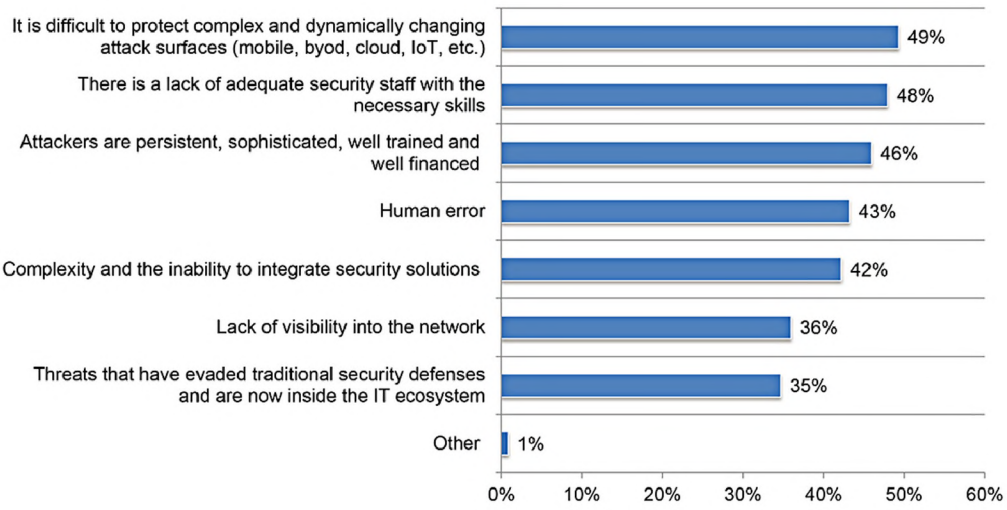
> Complex threats, staff shortages and disruptive technologies like IoT … this is a perfect storm for all sorts of bad things to occur if you are not staying one step ahead.
>
> *Dr. Larry Ponemon*

In its study *Closing the IT Security Gap with Automation: AI in the Era of IoT*, the Ponemon Group found that:

- 67% of security teams **attributed security gaps to the lack of visibility and control** into all the activity of everyday users and devices connected to the IT infrastructure.
- 62% of respondents said there were **gaps in the IT security infrastructure** that allow for penetration by attackers.

These overarching issues were broken down further into various root causes explaining how the gaps develop and lead to data breaches.

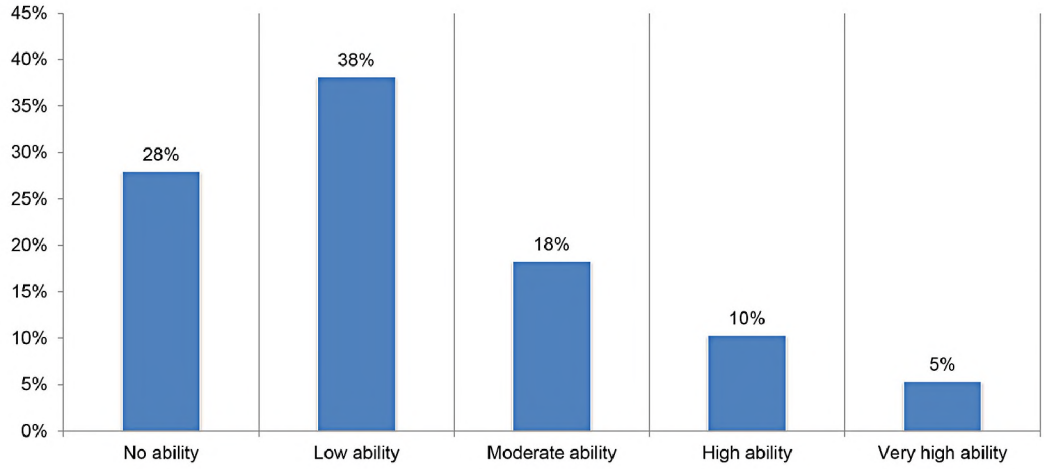
Figure 1: How the IT Security Gap Enables Data Breaches



IoT is widening the gap, straining standard and conventional security approaches.

As IoT devices grow increasingly common, even for simple monitoring tasks, 77% of security teams see these devices as a significant security threat. Standard and conventional security approaches don't always apply to IoT devices and applications, further widening the security gap. As a result, two-thirds of survey respondents reported having have "no ability" or "low ability" to secure IoT devices and apps.

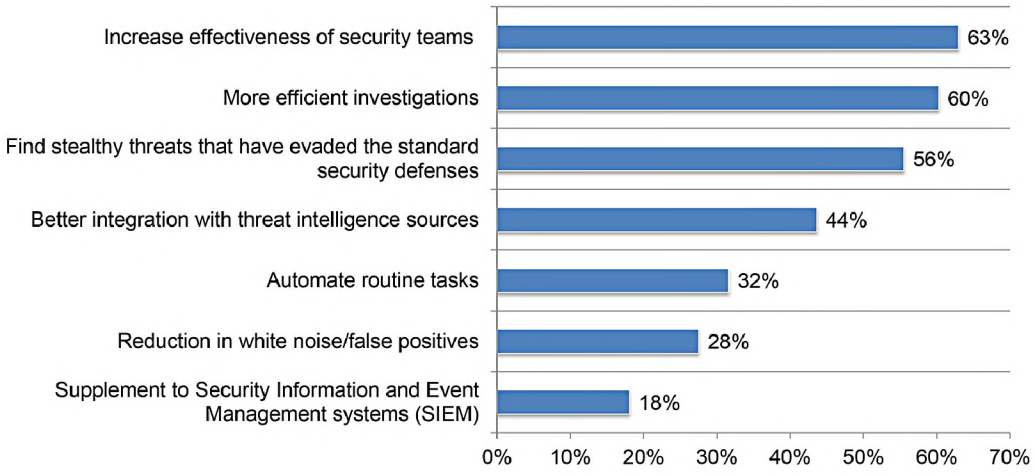
Figure 2: Ability to Secure IoT Devices and Apps



Despite current IoT security challenges, progress toward improving IoT security is still slow as companies grapple with understanding how to secure a rapidly expanding installed base of IoT devices and applications.

Artificial intelligence (AI) and machine learning (ML) both play a critical role in this regard, alongside traditional automation and other technologies, like network access control (NAC). Detecting evasive or "stealthy" threats, accelerating investigations, and overall security team effectiveness were seen as the top benefits of machine learning and advanced analytics.

Figure 3: Top Security Benefits from Machine Learning (ML) and Advanced Analytics



Organizations see the third-party IoT risk, but are behind in managing it.

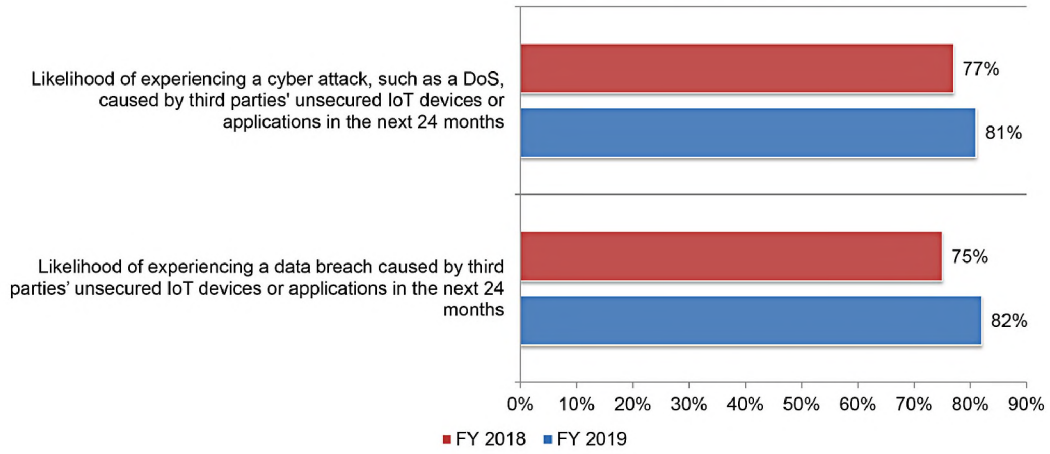
Unsecured third-party IoT devices and applications represent their own major threat to IoT security and risk management. The third annual study sponsored by the Santa Fe Group's Shared Assessments, *Third Party IoT Risk*, revealed that organizations are still facing an enormous readiness gap in IoT security.

What organizations do not know about IoT risks

- Lack of knowledge around how many cyber attacks, data breaches, and service disruptions have actually occurred
- Lack of knowledge about whether security safeguards and practices are adequate to mitigate IoT risk
- Lack of assigned accountability for IoT and the associated risk
- Lack of visibility about how and where IoT devices are inventoried
- Inadequate IoT risk assessment and control techniques
- Minimal understanding of third-party IoT risk management practices and policies
- Lack of training and awareness programs to address risks
- Lack of practitioners and third parties who fully understand IoT risks.

The study found that an overwhelming majority of respondents expect unsecured third-party IoT devices or applications to cause a data breach or cyber attack within the next 24 months.

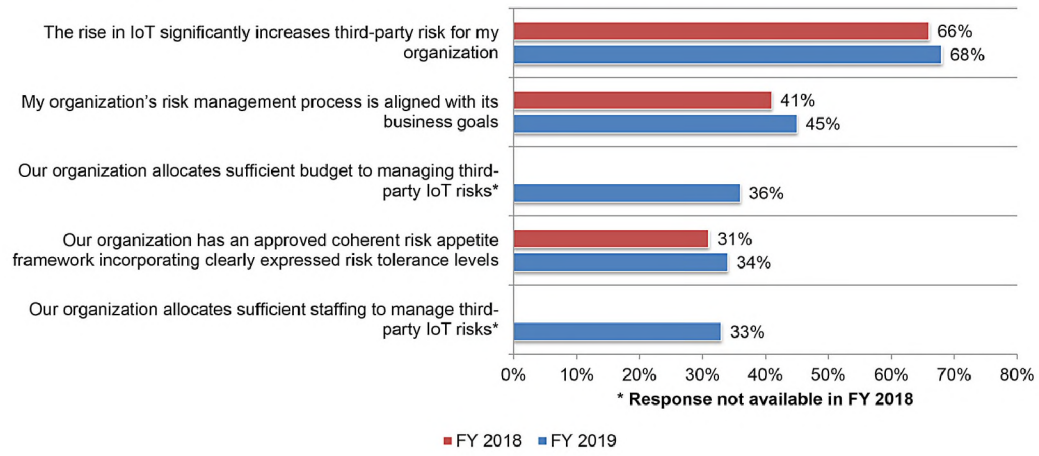
Figure 4: How likely is it that your organization will have a data breach or cyber attack caused by a third party's unsecured IoT devices? (Very Likely, Somewhat Likely, and Likely responses combined.)



Despite the widely recognized concern over IoT's third-party risks, governance and management of the threat is still weak in many organizations. Depending on the criteria, only 33-45% of the study's respondents agreed that their organization is prepared to meet the challenge (Fig. 5).

The results of a poll during the webinar strongly aligned with the study's results. For the statement, *"Our organization can appropriately secure IoT devices with our current security strategy,"* 29% agreed while 71% disagreed.

Figure 5: Perceptions about governance and management of third-party IoT risks



Start laying the right foundation now to manage the growing IoT cybersecurity challenge.

IoT security teams need to be watchful, recognizing that the threat is real and will continue to evolve. Although gaps will change as the technology and environment changes, organizations can begin laying a strong foundation to meet the challenge by taking these initial steps:

- **Assess the current state of IoT security** by taking an inventory of the organization's IoT devices and the sensitive and confidential information that resides on these devices.
- **Develop a plan to resolve imminent threats** and execute the plan with urgency. Have an incident response plan in place.
- **Engage leadership to make cybersecurity a priority** and communicate the risks and the state of security to them on a regular basis.
- **Develop and execute a communication strategy** to raise awareness and educate employees, especially privileged users.
- **Establish a project or taskforce** to tackle the third-party issue head on.
- **Set a strategic plan** for leveraging today's technologies, such as NAC and endpoint security, to mitigate the risk.
- **Engage with the right internal and external partners** in IoT and cybersecurity—do not go it alone!

> The security threat is real and, unfortunately, likely to evolve and become even worse from a damage control point of view.
>
> *Dr. Larry Ponemon*

BIOGRAPHY

Larry Ponemon, Ph.D.
Chairman and Founder, Ponemon Institute

Dr. Larry Ponemon is the Chairman and Founder of the Ponemon Institute and is considered a pioneer in privacy auditing and the Responsible Information Management or RIM framework. Dr. Ponemon was appointed to the Advisory Committee for Online Access & Security for the United States Federal Trade Commission. He was appointed by the White House to the Data Privacy and Integrity Advisory Committee for the Department of Homeland Security. Dr. Ponemon was also appointed to two California State task forces on privacy and data security laws. He is a member of Shared Assessments' Advisory Board.

Dr. Ponemon earned his Ph.D. at Union College. He has a Master's degree from Harvard University and attended the doctoral program in system sciences at Carnegie Mellon University. Dr. Ponemon earned his Bachelors with Highest Distinction from the University of Arizona, Tucson, Arizona. He is a Certified Public Accountant and a Certified Information Privacy Professional.