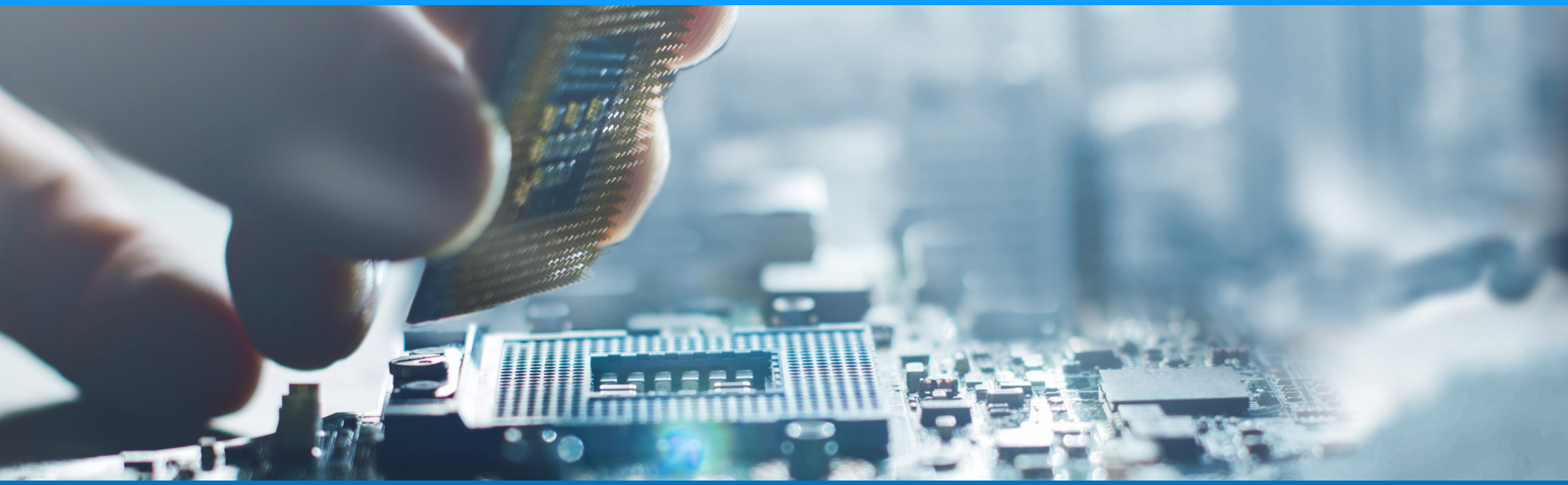
State of IoT Security Survey 2018



digicert®

MACHINES ARE TAKING OVER

Today there are nearly three devices attached to the internet for every human on the planet. By 2025 that ratio will soar to 10 to 1.[1] We live in an era where all manner of devices are finding their way online, such as thermostats, sensors in your car, medical devices, smart meters from your energy provider or complex equipment in industrial plants. Many refer to this move to connect everything as the "Internet of Things (IoT)."

Why is the IoT exploding? Sometimes it is as simple as reducing costs, such as how smart meters reduce the labor associated with meter reading. But a bigger driver is the digital transformation (DX) wave sweeping businesses. DX strives to optimize the customer experience during important "moments that matter," and IoT offers a way to do just that. Devices can monitor the customer experience and effect immediate changes in a way previously impossible for companies.

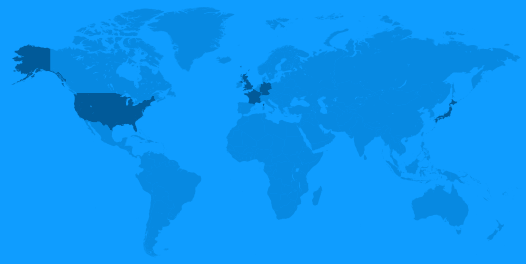
There are, however, risks. A world with 80 billion connected devices[2] is a world with a massively increased threat surface. We already see massive DDoS attacks driven by IoT devices, but experts say that is just the tip of the iceberg.[3] Security researchers continue to demonstrate vulnerabilities in common devices in use today.

Here at DigiCert we secure more than 26 billion internet connections every day and are constantly adding to that total as we onboard large IoT security deployments for our customers. So, we have more than a passing interest in how IoT will play out. In order to examine how enterprises globally are handling security as they embrace IoT, DigiCert commissioned ReRez Research of Dallas to execute a global survey of 700 organizations. What we found is a wake-up call for companies adopting IoT strategies.

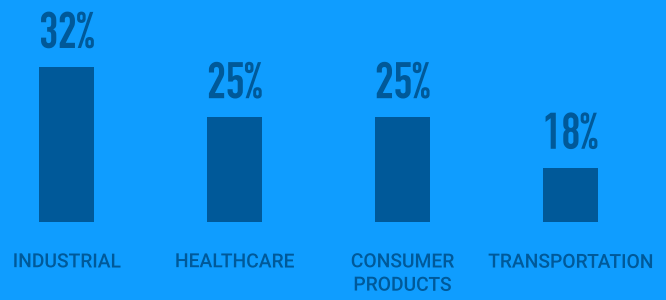
[1] IDC research, United Nations population forecasts
[2] IDC research
[3] IoT Security in the Spotlight

METHODOLOGY

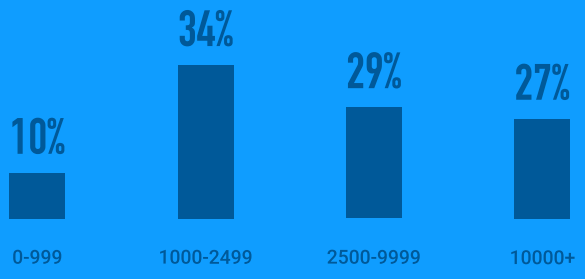
In September of 2018, ReRez Research fielded an online survey of 700 organizations in five countries around the world.



They focused on four industries known for early IoT adoption.



Company sizes ranged from very small to very large, with the median size being 3,000 employees.



IOT SECURITY MATTERS

Among companies struggling the most with IoT security, 25 percent reported IoT security-related losses of at least $34 million in the last two years. That number is only likely to grow with deployments unless changes are made. Why are these missteps occurring and what are the practices of companies performing better with IoT security? We explore these questions in this report.

We found strong interest in IoT. Eighty-three percent say IoT is somewhat to extremely important to their business today. That increases to 92 percent when asked about how important IoT will be by 2020. Yet it is early days: Just a third report that they have completed implementing their IoT strategy. Most are just getting started.

92% of companies say IoT will be important to their business in 2020.

Why are enterprises so interested in IoT? The top four goals enterprises report they are trying to achieve are:

- Increase operational efficiency
- Improve their customers' experience
- Grow revenue
- Achieve business agility

IOT ISN'T EASY: CONCERNS

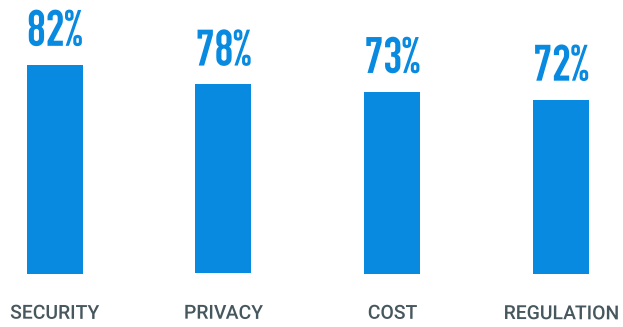
It turns out that enterprises are worried about IoT. The top four concerns enterprises report for IoT are:

Security
Cost
Privacy
Regulations

When we next explored the specifics of how enterprises are faring with their IoT efforts, we noticed big differences. Some enterprises are doing quite well, while others are struggling. As we contrasted the companies having the most success with IoT security with those struggling the most, we discovered eye-opening insights.

To tease out the differences we performed sophisticated cross-tabulations (See sidebar on the following page for a full explanation of how we did this). What we found provides solid lessons for enterprises as they embark on their IoT rollouts.

Top 4 Enterprise Concerns for IoT



SEPARATING THE BEST FROM THE WORST

There was a wide range of variation regarding how well enterprises are faring in terms of IoT security. To better understand what is fueling success for those who are doing well, DigiCert divided out survey results into three tiers:

TOP-TIER

These are the enterprises which are having the least problems with IoT security issues. They are much less likely to report having trouble mastering specific aspects of IoT security and reported far fewer problems.

MIDDLE-TIER

These are the enterprises which scored in the middle in terms of their IoT security results.

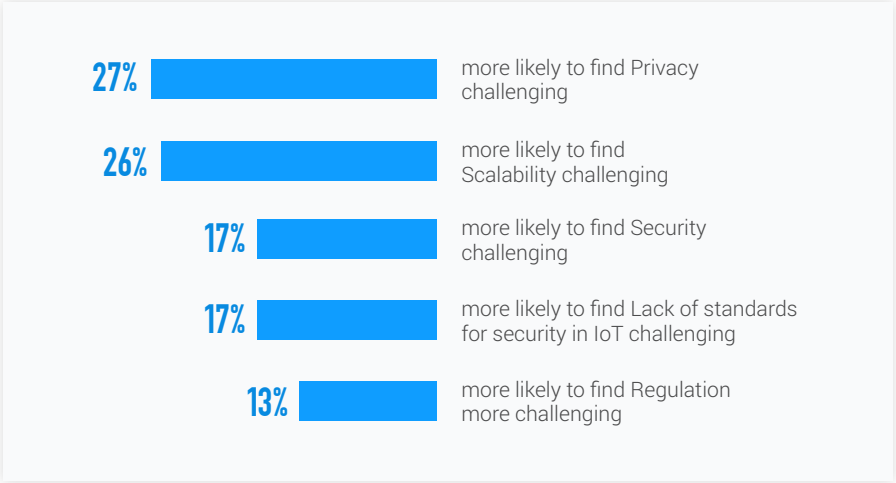
BOTTOM-TIER

These are the enterprises which are having the most problems with IoT security issues. They are much more likely to report having trouble mastering specific aspects of IoT security and reported far more problems.

IOT-RELATED SECURITY CHALLENGES AND MISSTEPS

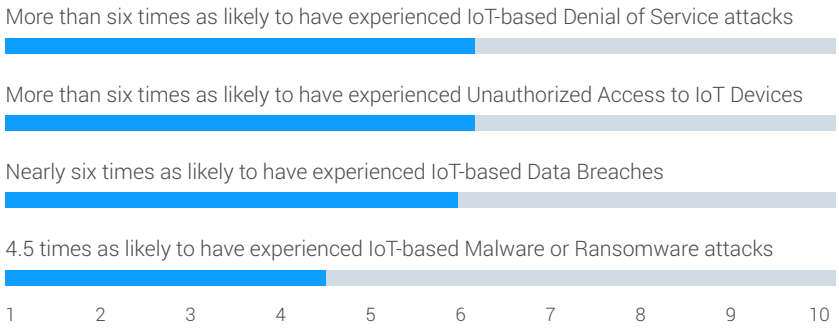
We asked our respondents to rate various IoT-related security issues in terms of how challenging each aspect was. We found dramatic differences between how bottom-tier and top-tier enterprises rated these security aspects. The bottom-tier enterprises were significantly more likely to report these items as being challenging.

Bottom-tier enterprises were **38 PERCENT MORE LIKELY** than top-tier enterprises to rate **Lack of appropriate IoT security-specific skillsets within their organization** as somewhat to extremely challenging.



We were curious if these challenges resulted in actual security missteps. This was precisely the case. We saw dramatic differences in IoT-related security missteps. In fact, only one third (32 percent) of top-tier enterprises experienced any incidents at all, whereas 100 percent of bottom-tier enterprises experienced at least one incident.

100% of bottom-tier enterprises experienced at least one incident.



We followed up on these missteps by asking how much each type of mishap cost the organization over the past two years.

25% of the bottom-tier enterprises reported IoT security-related losses of at least **$34 MILLION** in the last two years.

The most expensive damages came from five areas:

59%	MONETARY DAMAGES
59%	LOST PRODUCTIVITY
43%	LEGAL/COMPLIANCE PENALTIES
40%	LOST REPUTATION
31%	STOCK PRICE

PRACTICES OF THE TOP-TIER

With the markedly superior performance of top-tier enterprises, we were curious to explore their specific IoT-related security practices. Although the top-tier enterprises experienced some security missteps, an overwhelming majority reported no costs associated with this those missteps. The most common security practices the top-tier engaged in were:

Encryption of sensitive data

Ensuring the integrity of data being transmitted to or from a device

Scaling your security measures

Securing over the air updates

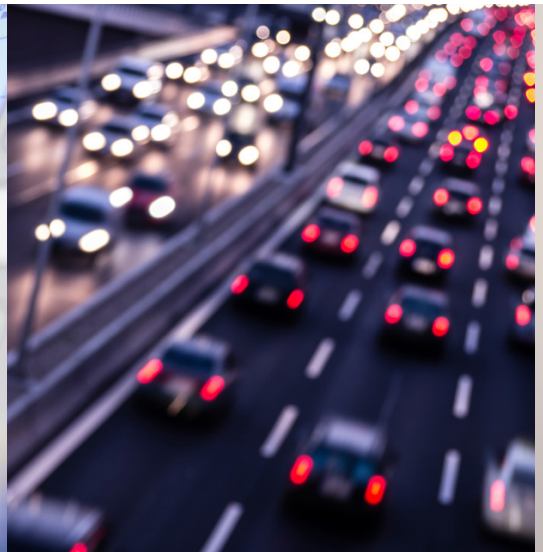
Secure software-based key storage

SECURING THE IOT EXPLOSION

As we gear up for a future with 80 billion IoT devices, we need to pay close attention to IoT security. The top-performing enterprises are drilling down on authentication and identity, encryption, and data integrity. DigiCert has a long and deep history with securing online connections and offers five best practices to help companies pursuing IoT succeed with their IoT security programs:

1. **Review risk**: Perform penetration testing to assess the risk of connected devices. Evaluate the risk and build a priority list for addressing primary security concerns, such as authentication and encryption. A strong risk assessment will help assure you do not leave any gaps in your connected security landscape.
2. **Encrypt everything**: As you evaluate use cases for your connected devices, make sure that all data is encrypted at rest and in transit. Make end-to-end encryption a product requirement to ensure this key security feature is implemented in all of your IoT projects.
3. **Authenticate always**: Review all of the connections being made to your device, including devices and users to ensure authentication schemes only allow trusted connections to your IoT device. Using digital certificates helps to provide seamless authentication with binded identities tied to cryptographic protocols.
4. **Instill integrity**: Account for the basics of device and data integrity to include secure boot every time the device starts up, secure over the air updates, and the use of code signing to ensure the integrity of any code being run on the device.
5. **Strategize for scale**: Make sure that you have a scalable security framework and architecture ready to support your IoT deployments. Plan accordingly and work with third parties that have the scale and expertise to help you reach your goals so that you can focus on your company's core competency.






digicert®

Connect with us on LinkedIn by searching “DigiCert”

Follow us on Twitter @digicert

www.digicert.com