

The background of the top half of the image is a dark blue gradient. On the left, there is a glowing blue globe showing the Americas. The rest of the background is filled with a complex network of light blue lines, nodes, and icons, including padlocks, arrows, and data symbols, representing a digital or cybersecurity theme.

Cybersecurity Forum 2020

The Threats to You, Your Company and the
Economy & Complying with the Cybersecurity
Maturity Model Certification (CMMC) Standards



Addressing the education and development needs of Florida's business community.



Chairman, Foundation of AIF

Jose Gonzalez
Director, Government
& Industry Relations
Walt Disney Parks
& Resorts

A Message from the Chairman

Whether you are seeking a “best practices” approach to providing cybersecurity or will be required to meet the new federally mandated standards, this series of educational offerings provide an ever-changing model for responding to real cybersecurity risks that seemingly involve all aspects of our society. Regardless of your profession (risk managers, safety professionals, HR professionals, company managers, IT specialists, attorneys, etc.) or whether you represent individuals, provide services or are a vendor for public or private corporate interests, this Forum Series will be of significant value to you.

Cybersecurity has become a major part of any Risk Management Program. It is not for the sole concern of a company’s IT department; rather, it is “everyone’s problem” within the business and needs everyone’s attention. For those seeking updated technical information on the new defense “supply chain” mandatory cybersecurity requirements, professionals responsible for their development and use by their industry will be addressed.

On September 16-17, 2020, FAIF hosted the second annual Florida Cybersecurity Forum [virtually](#) which convened leading cybersecurity experts from around the country, business executives and senior elected officials. The Forum had more than 150 representatives from various industries, state and local governments, academia, and the media in attendance.

Cybersecurity Forum 2020

The Foundation of Associated Industries of Florida partnered with FloridaMakes, the Florida Department of Economic Opportunity, the Workers' Compensation Institute, and the U.S. Department of Defense Office of Economic Adjustment in September of 2020 to present the second annual Florida Cybersecurity Forum.

This unique partnership provided an extremely well-rounded discussion of how the critical issue of cybersecurity affects all manner of businesses in the state of Florida.

Panels at the Forum included:

- **The Long View on Cybersecurity**
- **The Legal and Personal Financial Risks of Cyber Breaches**
- **Cyber Breach** – The Real Thing and Its Expected Impact
- **Are We Prepared for a National Crippling Cyber-attack?** Lessons Learned from the Pandemic Crisis
- **Cybersecurity and the Space Industry:** Introduction to CMMC, the New Cybersecurity Standards
- **Perspectives from the CMMC Accreditation Body**
- **CMMC Challenges and Opportunities** – How will CMMC Affect the Florida Economy?

Key Speakers included:

- **U.S. Senator Marco Rubio**
- **Katherine “Katie” Arrington** – Chief Information Security Officer for Acquisition and Sustainment to the Under Secretary of Defense for Acquisition and Sustainment
- **Congressman Michael Waltz**
- **Florida CFO Jimmy Patronis**
- **Beverly Seay** – Senior Executive with global experience and a Fortune 500 track record and is currently an advisor for the National Security Innovation Network.

Once thought to be a concern of only the large organizations, cyberattacks are presently a threat to the existence of every business in the state of Florida. Businesses have progressed in the last few decades to a total dependence on interconnected devices, many of which are the backbone of day-to-day operations. Their vulnerability and risk are a direct reflection of our reliance on computers and connection. If a company utilizes the internet in any manner, there is a risk of a cybercrime — no matter the size




of the company. In terms of cybercrimes, large corporation data breaches such as those at Target, Home Depot, and Equifax often come to mind. However, security breaches affect all levels of businesses, as today nearly 50% of small businesses have been subjected to a cyberattack.

As we have moved further into the cyber age, nefarious actors have adapted to overcome cybersecurity safeguards in place. In the case of Home Depot, cybercriminals gained access to secure data with a simple phishing scam — a phony invoice embedded with malware. Many believe their company is safe from a malicious attack, and the company itself may be, but the vendors who make up a company's supply chain may be the weak links. In the case of Target's data breach where commodity malware was used to breach the vendor portal, it exploited the relationship between a vendor and Target thereby gaining access to the desired data. Supply chain security is only as strong as the weakest link.

Consider the extensive volume of data stored on any one network: personal files, banking and insurance information, medical records, legal documents, intellectual property and more. When evaluating potential risk, companies must ask themselves: what is the value (cost) of data stored on the computers and what is the cost to the business if the network goes down and goods are unable to be produced? The subject matter of stored data is of paramount importance when considering the probability of a cyberattack. Medical records, for instance, can fetch \$1,000

Once thought to be a concern of only large organizations, **cyberattacks are presently a threat to the existence of every business in the state of Florida.**

50% 

Nearly **50%** of small businesses have been subjected to a cyberattack.

A company itself may be safe from a malicious attack, but **the vendors** who make up a company's **supply chain** may be the **weak link**



- The **cost of a breach has doubled** since 2007
- The average cost of a healthcare-related breach is **\$7.13 million**
- Small companies spend an average of **\$200,000 per attack**
- **60%** of businesses permanently close within 6 months of an attack

Cyberattacks are here to stay and will continue to get more complicated and difficult for businesses to navigate.



The Legal and Personal Financial Risks of Cyber Breaches Panel

Moderator:

Julie Fetherman
Workers' Compensation Institute

Panelists:

Commissioner David Altmaier
Florida Office of Insurance Regulation

Michelle Chia, Esq.
Zurich North America

Robert A. Stines, Esq.
Freeborn & Peters, LLP

per record on the dark web. When a manufacturer faces a breach and loses access to network files, how long they can continue to produce goods not only affects the business, but sends ripples down the supply chain.

In addition to the loss of sensitive personal data, the cost of a breach has doubled since 2007. The Home Depot and Target breaches came with a nearly \$200 million price tag. The average cost of a healthcare-related breach is \$7.13 million. Small companies spend an average of \$200,000 per attack, and 60% of businesses permanently close within 6 months of an attack. These hard numbers are indicative of just how costly a data breach can be. The cost increase can be attributed to the multitude of issues an organization must resolve after a post-data breach such as client notification, entry point investigation, litigation, penalties, fines and ultimately business interruptions. In fact, malicious actors can not only harvest data, but can also inflict kinetic attacks on infrastructure, rendering equipment such as generators entirely unusable.

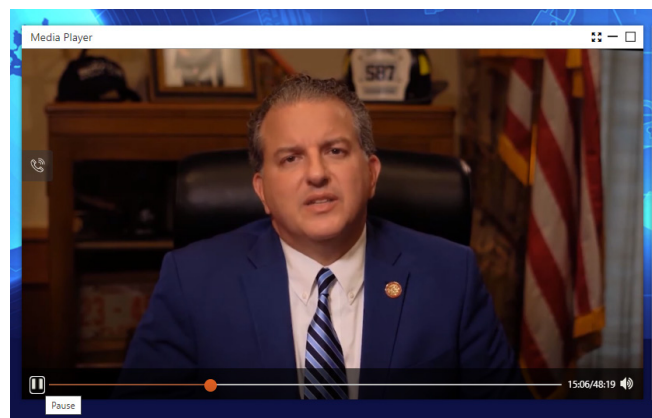
Corporate data breaches and kinetic attacks have lasting negative impacts. With a network of over 350,000 companies and subcontractors, the Department of Defense (DoD) has recently taken steps to ensure the hardening of the DoD supply chain by introducing the Cybersecurity Maturity Model Certification (CMMC). This Certification verifies that contractors have adequate cybersecurity controls and policies in place to meet the security standards of the military. This system ensures government contractors can defend against current and future cyberattacks in a proactive manner.

Going forward, companies must adopt a zero-trust mentality. Employers must expect that an adversary has already found a way to compromise their security and take actions to mitigate the risk that a cybercriminal's existence presents. Cyber adversaries do not have rules and they are extraordinarily adaptive; thus, cybersecurity requires a proactive approach. It requires us to look ahead and enact preventative measures to avoid security breaches. The best approach to handle a cyberattack is to implement policies, procedures and tools to prevent it from occurring.

One overwhelming consensus of all speakers and participants of the Forum was that this issue is here to stay and will continue to get more complicated and difficult for businesses to navigate. Ongoing discussion and collaboration between the private and public sectors will be crucial moving forward as workable and affordable solutions are implemented.



U.S. Senator Marco Rubio



Florida CFO Jimmy Patronis



Christopher P. Cleary, PMP, CISSP
Chief Information Security Officer
Department of the Navy

The Foundation of Associated Industries of Florida (FAIF) was formed to address the education and development needs of Florida's business community. FAIF fosters programs that identify business needs today and create solutions that will last into the future.

FAIF focuses on current issues that are important to the success of Florida employers, and works to educate the public at large about these issues to make Florida a better place for its businesses and citizens to call home.

