OFIaWARN

Cyber Security

Jonathan Kilpatrick, CEO Trulight LLC 850-270-3053 Jim Mcclaugherty FRWA 850-668-2746



"RISK & RESILIENCE" VULNERABILITY ASSESSMENT

AMERICAS WATER INFRASTRUCTURE ACT OF 2018 (AWIA). THE WATER RESOURCES DEVELOPMENT ACT (WRDA BILL) WAS SIGNED INTO LAW BY PRESIDENT TRUMP ON OCTOBER 23, 2018.

ASSESSMENT REPORT DOCUMENTS WERE BEING DRAFTED BY FRWA AS DIRECTED BY THE FLORIDA DEPARTMENT OF ENVIRONMENTAL PROTECTION IN ORDER TO HELP WATER SYSTEMS ABOVE 3300 POPULATION SERVED TO ACHIEVE COMPLIANCE. THE PILOT STUDY BEGAN IN SEPTEMBER OF 2018, ONE MONTH PRIOR TO THE SIGNING OF THE WRDA BILL.

CYBER SECURITY CONCERNS ADDRESSED: 1: PENETRATION TESTS PERFORMED 2: SOCIAL ENGINEERING/PHISHING TEST (HACKING COMPUTER SYSTEMS)

PENETRATION TESTS OF 5 RANDOMLY SELECTED UTILITIES, OUT OF THE 5 UTILITIES, 2 PLANTS RESULTED IN PENETRATION TEST RESULTS OF ENTRY TO THEIR SCADA SYSTEMS. THIS SMALL SAMPLE SIZE RESULTED IN 40% OF THE UTILITIES TESTED HAD VULNERABILITIES THAT ALLOWED A BREACH TO THEIR NETWORK PERIMETER.

WHAT MADE ONE PARTICULAR ASSESSMENT A VERY STRATEGIC OUTCOME WAS DUE TO THE FACT THAT A THIRD PARTY COMPANY THAT PROVIDES THE SCADA PACKAGE WAS VERY KEEN ON THE OUTCOME. THEY ARE A MANAGED SCADA COMPANY AND THEY WERE VERY PROACTIVE AS THEY PROVIDE PACKAGED SYSTEMS ALL OVER THE COUNTRY. THERE WERE 8 VULNERABILITIES IDENTIFIED THAT COULD BE EXPLOITED INTO THE SCADA SYSTEM AND THE COMPANY IMMEDIATELY STARTED ON A COURSE OF REMEDIATION.

THESE VULNERABILITIES WERE SUMMARIZED IN A FINAL REPORT FOR THE FDEP AND FOR THE THIRD PARTY COMPANY. THEY COMPLETED THE COURSE OF REMEDIATION FOR ALL OF THEIR SYSTEMS BY MAY 1, 2019, SO FLORIDA SYSTEMS AND SYSTEMS ALL OVER NORTH AMERICA ARE NOW BETTER PROTECTED FROM CYBER INTRUSION.

SECURITY MEASURES

1. BACK UP AND RESTORE:

THE MOST IMPORTANT PART OF YOUR STRATEGY IS TO DO REGULAR DATA BACKUPS

2. UPDATE AND PATCH:

MAKE SURE YOUR SECURITY SOFTWARE AND PATCHES ARE UP TO DATE ON ALL DEVICES. THIS SOUNDS EASY ENOUGH BUT MOST IT PROFESSIONALS WILL ADMIT THAT THEY STRUGGLE TO KEEP UP WITH THE SHEER VOLUME OF PATCHES THAT ARE RELEASED EVERY MONTH.

3. TRAIN AND EDUCATE:

MOST RANSOMWARE ATTACKS BEGINS WITH A SINGLE WELL-INTENTIONED EMPLOYEE OPENING WHAT APPEARS TO BE A WORK RELATED EMAIL. CYBER CRIMINALS ACTIVELY EXPLOIT HUMAN ERROR AND CURIOSITY. THE RANSOMWARE EMAIL IS DESIGNED TO FOOL HUMANS INTO BECOMING UNWITTING ACCOMPLICES AND TYPICALLY PLAYS ON THE USERS LACK OF AWARENESS AND REQUIRING THEM TO OPEN MALICIOUS WORD DOCUMENT ATTACHMENTS AND ENABLE MACROS.

4. FBI STATISTIC:

A 2020 REPORT SHOWED 69 % YEAR OVER LAST YEAR INCREASE IN CYBERCRIME COMPLAINTS.

DIRECTIVE FROM ANNE NEUBERGER, DEPUTY ASSISTANT TO THE PRESIDENT AND DEPUTY NATIONAL SECURITY ADVISOR FOR CYBER AND EMERGING TECHNOLOGY: DATED JUNE 2, 2021

FIVE BEST PRACTICES

- BACKUP YOUR DATA, SYSTEM IMAGES AND CONFIGURATIONS REGULARLY TEST THEM AND KEEP THE BACKUPS OFFLINE.
- 2. UPDATE AND PATCH SYSTEMS PROMPTLY.
- 3. TEST YOUR INCIDENT RESPONSE PLAN:
- 4. CHECK YOUR SECURITY TEAM'S WORK
- 5. SEGMENT YOUR NETWORKS.

Cyber Security FlaWARN

JONATHAN KILPATRICK, CEO TRULIGHT LLC

- FORMER CIO FOR CITY OF TALLAHASSEE
- CYBER SYSTEMS OFFICER FOR FLORIDA AIR NATIONAL GUARD
- OVER 30 YEARS IN TECHNOLOGY



Cyber Security FlaWARN

JONATHAN KILPATRICK, CEO TRULIGHT LLC

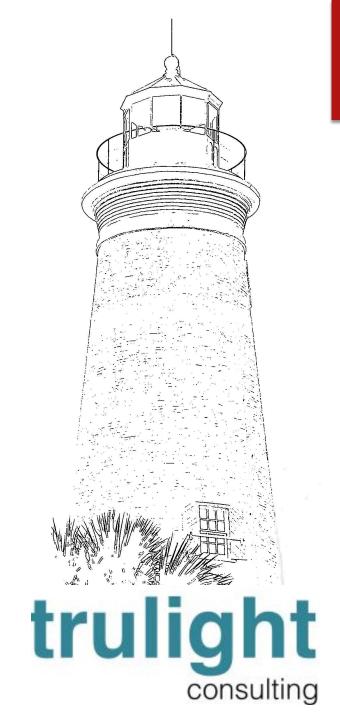
- FORMER CIO FOR CITY OF TALLAHASSEE
- CYBER SYSTEMS OFFICER FOR FLORIDA AIR NATIONAL GUARD
- OVER 30 YEARS IN TECHNOLOGY



Trulight LLC

www.trulightconsulting.com

- ► Technology Strategy
- ► Cyber Security
- ▶ Compliance



What is this?



What is this?



What is this?



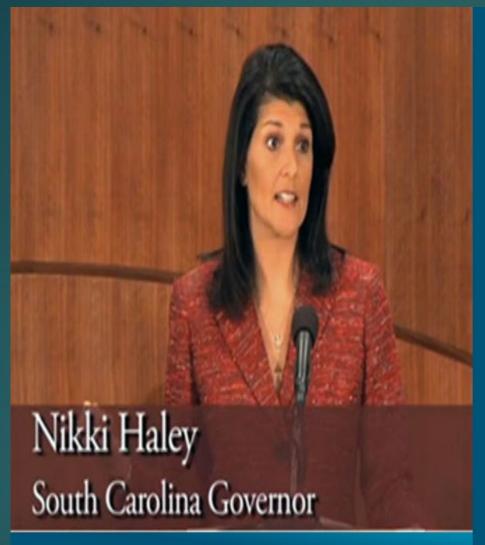
Threats

- All systems have vulnerabilities
- All systems have risks

Threats

- Thrill Seekers
- Criminal Organizations
- Nation State Sponsored

- Cyber crime cost businesses in the United States more than \$3.5 billion in internetrelated cyber crimes and damages according to a 2019 FBI report.
- The cost of cybercrime totaled more than \$1 trillion across the world last year (2021)
- Estimated Cost is 1% of Global GDP and growing at 50% per year



"...what we have to remember is those who attack are patient, and those that attack never stop trying.

So, if that's the case, we can never stop working to make sure we keep things safe. "

-- Governor Nikki Haley

Thrill Seekers

- Detectable
- Challenge
- Nuisance

Criminal

- Professionals
- Highly Trained
- Financially Motivated

Nation State

- Professionals
- Highly Trained
- Financial
- Nationalist Goals

Cyber Threat Trends

Threats are increasing:

Hacking tools are more readily available and simpler to use

The potential impact of cyber attacks continues to grow

Hacker motivation is changing:

No longer egocentric, hobbyist hackers seeking entertainment and internet status

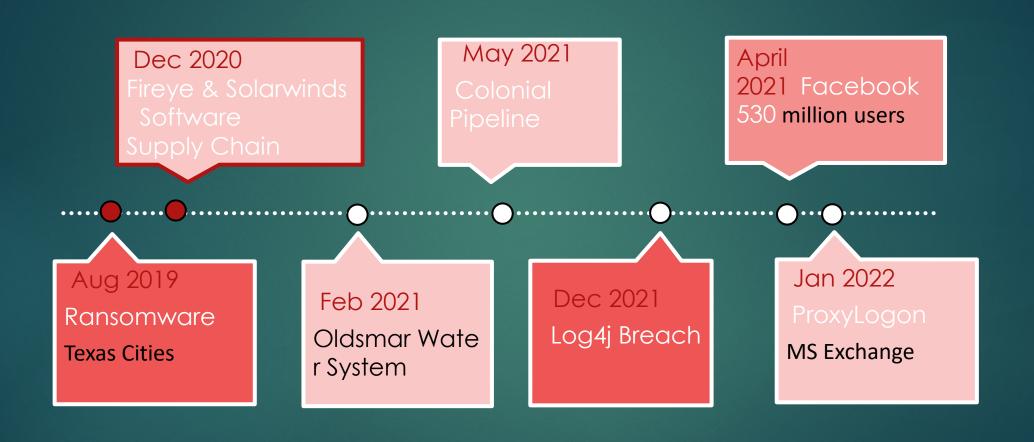
Shift to professional cyber criminals motivated by money whose success relies on remaining undetected

- Certain factors are enabling threat actor success:
 - Economy of organized cybercrime
 - Inter-connected systems
 - Widespread organizational failure to implement cyber hygiene

Nation State

- Very Quiet
- Data Extraction
- Disruption
- Financial Gain
- Intellectual Property Theft

Recent Well-Known Cyber Incidents



What is Cybersecurity?

The protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users

Safeguarding computer systems, as well as the data contained within, and maintaining:

- Confidentiality
- Integrity
- Availability

Prevention and Detection



Prevention and Detection

- Asset Management and Awareness
- Update all software
- Monitor for data anomalies
- Prepare for an incident
- Stay informed

Prevention and Detection

- Train Staff
- Assume you will have a breach
- Incident Response Plan

Preparation Cyber Security

- Penetration Testing
- Vulnerability Analysis
- 3rd Party Assessments
- Code Evaluation



Don't let this be you



Because...

Someone Somewhere Is penetration testing your systems



Thank You

Jonathan Kilpatrick
Trulight LLC
www.trulightconsulting.com
(850) 270-3053
Jonathan.Kilpatrick@trulightconsulting.com

