FORWARD
STRONGER TOGETHER

MOTOROLA SOLUTIONS:
IS YOUR COUNTY PREPARED FOR CYBER ATTACKS?

Taylor Johnson

Motorola Solutions, Cybersecurity Services

2022 Cybersecurity Summit

AGENDA

FORWARD
STRONGER TOGETHER

- Introduction
- Threats to Public Safety
- CISA Guidance
- Public Safety Cybersecurity Challenges
- How Can You Protect Yourselves Today?
- Q&A

MOTOROLA SOLUTIONS CYBER BACKGROUND

FORWARD
STRONGER TOGETHER

Recent Cybersecurity Acquisitions - Company History

- Founded in 2007 (US Based)
- 72 employees
- 50/50 Government/Commercial mix
- Product and Service Offerings
  - Technical/Non-Technical Assessments
  - Virtual CISO
  - Cyber Exercises and Training
  - Managed Security Services
  - Cloud Security Platform
- Support the Top Incident Response Firms
- Top Secret Facility Clearance
- Security Operations Centers in Texas and Virginia

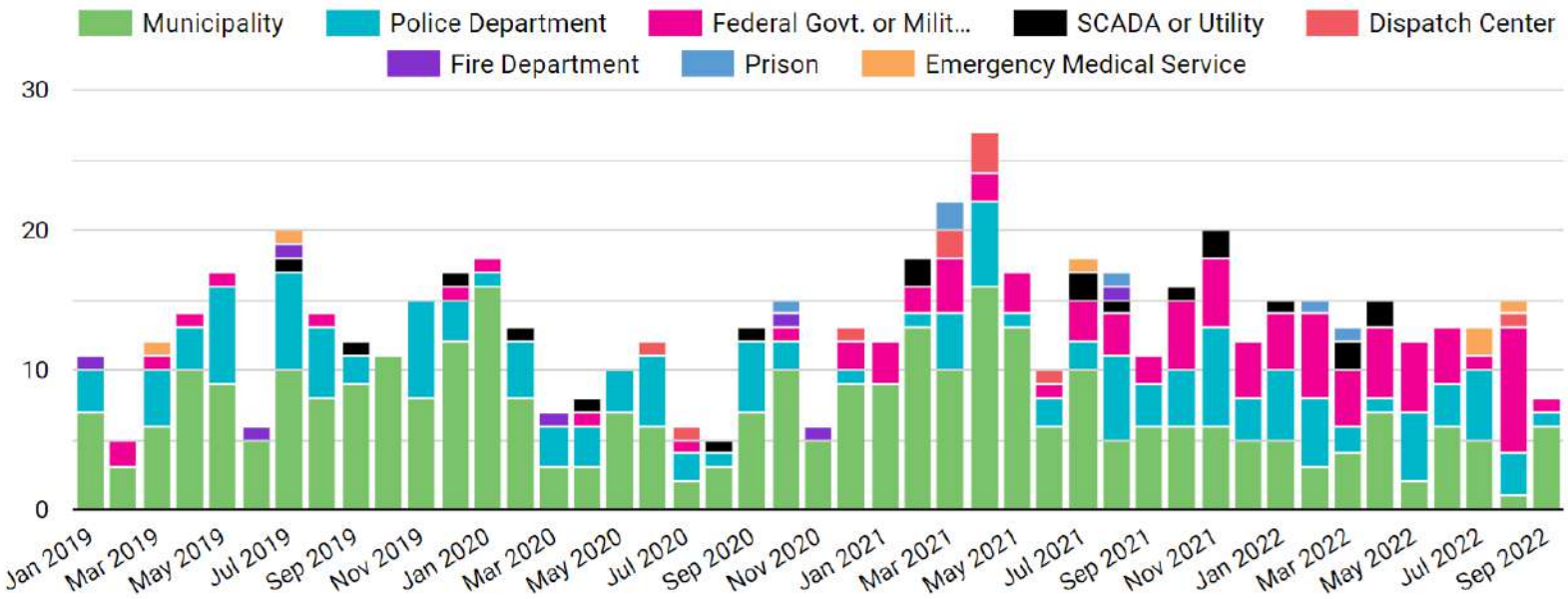
DELTA RISK

- Founded in 2004 (US Based)
- 118 employees
- 60/40 Government/Commercial mix
- Product and Service Offerings
  - Technical/Non-Technical Assessments
  - Cloud Architecture Consulting Services
  - Security Automation Solutions
  - Training and Certification (School of Cybersecurity)
  - Managed Security Services
- Top Secret Facility Clearance
- Security Operations Centers in Ohio and Virginia

LUNARLINE
SOLUTIONS BUILT ON SECURITY™

CYBER ATTACKS TO PUBLIC SAFETY

FORWARD
STRONGER TOGETHER



Year	2019	2020	2021	2022*
# of Cyber Attacks (% change from year prior)	154	126 (-18%)	199 (+58%)	119 (-17%*)

01 Jan. - 14 Sep 2022

CISA GUIDANCE FOR GOV'T SYSTEMS

SHIELDS UP Guidance for All Organizations

CISA recommends all organizations—regardless of size—adopt a heightened posture when it comes to cybersecurity and protecting their most critical assets. Recognizing that many organizations find it challenging to identify resources for urgent security improvements, we've compiled a **catalog of free services** from government partners, and industry to assist. Recommended actions include:

Reduce the likelihood of a damaging cyber intrusion

- Validate that all remote access to the organization's network and privileged or administrative access requires multi-factor authentication.
- Ensure that software is up to date, prioritizing updates that address **known exploited vulnerabilities identified by CISA.**
- Confirm that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes.
- If the organization is using cloud services, ensure that IT personnel have reviewed and implemented **strong controls outlined in CISA's guidance.**
- Sign up for **CISA's free cyber hygiene services,** including vulnerability scanning, to help reduce exposure to threats.

Take steps to quickly detect a potential intrusion

- Ensure that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior. Enable logging in order to better investigate issues or events.
- Confirm that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated.
- If working with Ukrainian organizations, take extra care to monitor, inspect, and isolate traffic from those organizations; closely review access controls for that traffic.

Ensure that the organization is prepared to respond if an intrusion occurs

- Designate a crisis-response team with main points of contact for a suspected cybersecurity incident and roles/responsibilities within the organization, including technology, communications, legal and business continuity.
- Assure availability of key personnel; identify means to provide surge support for responding to an incident.
- Conduct a tabletop exercise to ensure that all participants understand their roles during an incident.

Maximize the organization's resilience to a destructive cyber incident

- Test backup procedures to ensure that critical data can be rapidly restored if the organization is impacted by ransomware or a destructive cyberattack; ensure that backups are isolated from network connections.
- If using industrial control systems or operational technology, conduct a test of manual controls to ensure that critical functions remain operable if the organization's network is unavailable or untrusted.

PUBLIC SAFETY CYBERSECURITY CHALLENGES

CYBER THREATS INCREASING IN SCOPE, SCALE, AND COMPLEXITY

- General lack of end-to-end cyber threat intelligence and proactive defense capabilities
- All but the largest/most resourced organizations must focus on core functions (not cybersecurity)

INADEQUATE MONITORING

- Limited to core network assets while applications are exposed
- Lack of 24/7/365 support capabilities and global visibility/insights

LACK OF PERSONNEL

- IT/Safety personnel filling cyber roles and challenges to recruiting/retaining cybersecurity talent
- Knowledge base generally focused on internal network security versus cloud

REMOTE ACCESS

- Endpoints (mobile and external connected devices) create security gaps
- Home-based office use straining access security guidelines and lessening security protocols

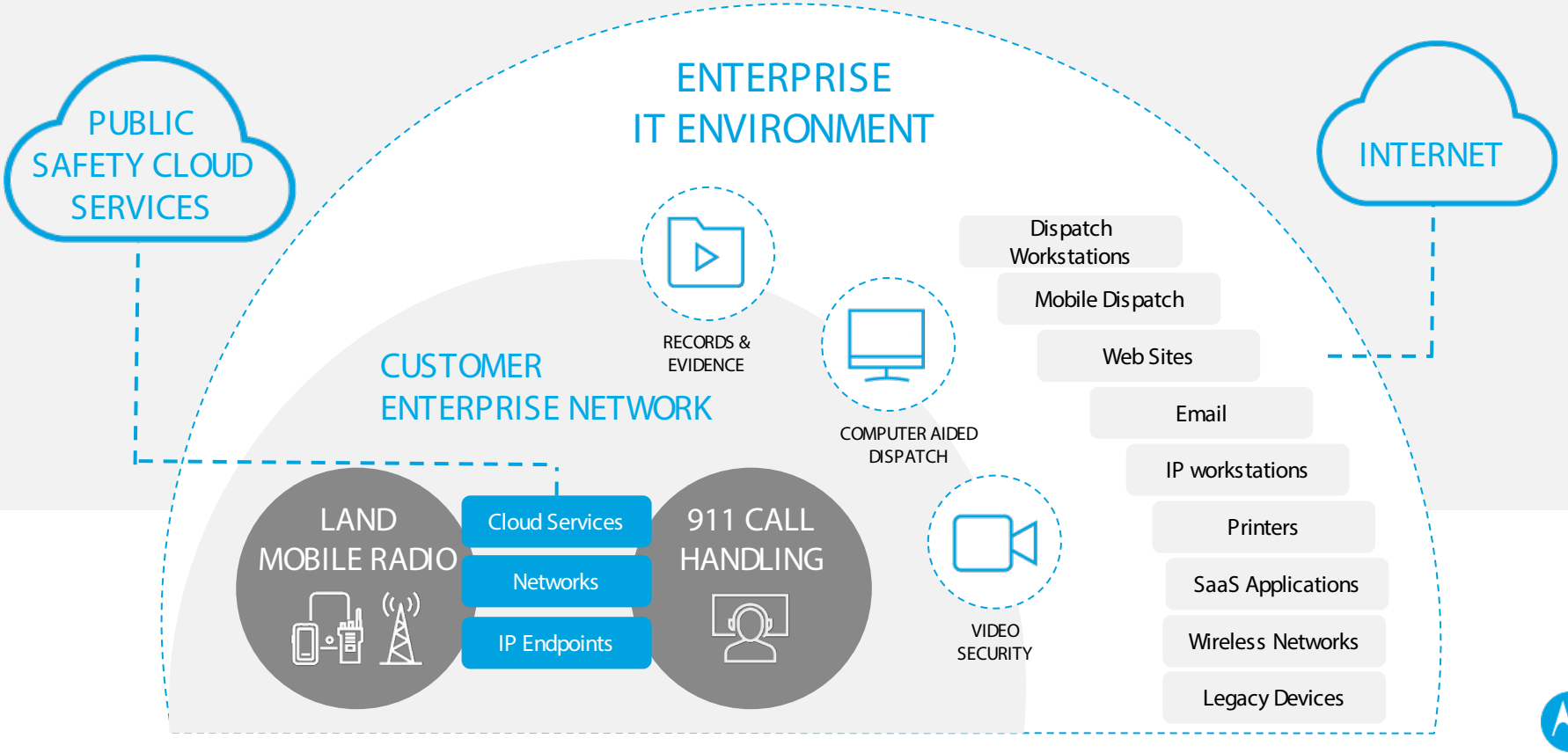
LACK OF PUBLIC SAFETY-FOCUSED INFORMATION AND INTELLIGENCE SHARING

- No dedicated Information Sharing and Analysis Organization/Center (ISAO/ISAC)
- Multiple information/intelligence feeds (ISACs, CISA, FBI, etc.) - Public Safety relevance?

THE PUBLIC SAFETY LANDSCAPE

What needs protection?

FORWARD
STRONGER TOGETHER



THERE IS NO SUCH THING AS A CLOSED NETWORK

FORWARD
STRONGER TOGETHER

- INSIDER THREAT
- EXTERNAL NETWORK CONNECTIONS
- UNAUTHORIZED CONNECTIONS
- BYOD AND MAINTENANCE LAPTOPS
- EXTERNAL DISC MEDIA AND USB DRIVES

SO WHAT WE DO ABOUT IT?

PUBLIC SAFETY CYBERSECURITY SOLUTIONS

INFORMATION/INTELLIGENCE COLLECTION

- Multiple external (public/private) feeds
- Information/intelligence from our Cybersecurity Services platforms

INFORMATION/INTELLIGENCE ANALYSIS AND SHARING

- Dedicated analysts
- Dedicated Threat Intelligence Exchange/Platform

PROACTIVE DEFENSE

- Managed Detection and Response (MDR) for 24/7/365 monitoring and support
- Professional Services including risk assessments, penetration testing, and tabletop exercises

ADVERSARY CAMPAIGN ANALYSIS AND MITIGATION

- Focused analysis on the most dangerous adversary campaigns targeting Public Safety
- Continuously updated playbooks, with technical indicators and preventive controls

WHAT CAN YOU DO TO PROTECT YOUR NETWORK

FORWARD
STRONGER TOGETHER

ACTIONABLE STEPS YOU CAN TAKE TODAY

1. KNOW YOUR NETWORK - Hardware, Software, Applications, Data Flows
2. KNOW YOUR ADVERSARY - Who is attacking you and how might they do it?
3. PATCH, PATCH, PATCH - This is not easy to execute operationally but it is essential
4. KNOW WHAT NORMAL LOOKS LIKE - The only way to detect abnormal
5. EDUCATE YOUR USERS - Cybersecurity is everyone's responsibility
6. KNOW HOW TO RESPOND TO A CYBER ATTACK - Train Hard, Fight Easy

FORWARD

STRONGER TOGETHER

THANK YOU