UC RIVERSIDE

Operational Technology Threat

Russia-Ukraine Tension Poses Cyber Threat to U.S.

February 08, 2022

UC RIVERSIDE
Office of Emergency Management

What's The Issue?

- According to The Center for Strategic and International Studies (CSIS) (1, 2):
  - Russia considers Ukraine becoming more integrated with NATO as a threat to its national security and has demanded that the military alliance does not expand eastward to Ukraine or other former Soviet states.
  - It has also demanded that NATO roll back its military deployments in Central and Eastern Europe.
  - Russia is pursuing a dual approach in Ukraine, combining a major buildup of conventional forces with clandestine irregular activities.
  - Moscow has prepared a growing number of its conventional military units for a possible invasion of Ukraine and organized its intelligence services to conduct extensive ***cyber operations, subversion, and sabotage.***
  - If peace talks fail, an escalation between NATO & Russia could extend well beyond Eastern Europe and include retaliatory measures that are ***global*** in nature.
  - While many experts believe that Russian forces are still several weeks away from being ready to mount a cross-border movement in force, this conflict, if it comes, will not likely not be confined to Ukraine. (3, 4, 5)
- As of 6 February 2022, intelligence officials assess that Moscow has 70% of its strike force in place for an attack that could happen at any moment over the next couple of weeks," (6, 7)

Note: the cyber threat doesn't run entirely in one direction. In addition to the prospect of NATO retaliatory or preemptive cyber operations, hacktivists could begin to hit Russian targets - the recent disruption of Belarusian rail transport by the Cyber Partisans illustrates that hacktivism might also surface in Russia.

Precedents: Russian Cyber Aggression

UC RIVERSIDE Office of Emergency Management

June 2021. Hackers linked to Russia's Foreign Intelligence Service installed malicious software on a Microsoft system that allowed hackers to gain access to accounts and contact information. The majority of the customers targeted were U.S. based, working for IT companies or the government.

June 2021. The U.S. and British governments announced the Russian GRU attempted a series of brute force access against hundreds of government and private sector targets worldwide from 2019 to 2021, targeting organizations using Microsoft Office 365® cloud services.

May 2021. The world's largest meat processing company, Brazilian-based JBS, was the victim of a ransomware attack. The attack shut down facilities in the United States, Canada and Australia. The attack was attributed to the Russian speaking cybercrime group, REvil.

May 2021. On May 6, the Colonial Pipeline, the largest fuel pipeline in the United States, was the target of a ransomware attack. The energy company shut down the pipeline and later paid a $5 million ransom. The attack is attributed to DarkSide, a Russian speaking hacking group.

March 2021. Polish security services announced that suspected Russian hackers briefly took over the websites of Poland's National Atomic Energy Agency and Health Ministry to spread false alerts of a nonexistent radioactive threat.

Please note that examples / activity involve a Russian-nexus, but not necessarily nation-state sponsored incidents.

What Does This Mean To The U.S.?

UC RIVERSIDE Office of Emergency Management

- The U.S. Cybersecurity and Infrastructure Security Agency released guidance describing the risks and identifying a number of steps that organizations should take to address their cybersecurity posture. (1, 2, 3)
- A January 23 DHS Intelligence and Analysis Bulletin stated:
  - "We assess that Russia would consider initiating a cyberattack against the Homeland if it perceived a U.S. or NATO response to a possible Russian invasion of Ukraine threatened its long-term national security."
- Experts are concerned that in the wake of recent cyberattacks by hackers affiliated with Russia, the Russian government has the capability to carry out disruptive and destructive attacks against targets in the U.S.
- The SolarWinds attack, uncovered in December 2020, gave the perpetrators access to the computer systems of many U.S. government agencies and private businesses.
- The DHS and FBI accused Russian hackers in March 2018 of infiltrating U.S. energy and infrastructure networks.

In December 2015, Russian hackers knocked out power to 225,000 customers of the regional power companies in Ukraine's Ivano-Frankivsk region. This was the first publicly acknowledged cyber attack that resulted in power outages and was a sophisticated attack by well-resourced threat actors. Hackers used spearphishing to gain access to the power company's network, implanted BlackEnergy and KillDisk malware to gain control of the systems controlling the power grid, and then issued commands – by taking over the operators' mouse controls -- that resulted in shutting down the system and making it inoperable. Operators had to restore the system manually, a process that took several days. The hackers compounded the problem by generating thousands of telephone calls to the power company's call center, making it impossible for customers to report outages and for the company to understand the extent of the problem. This successful attack was followed by an even larger attack on Ukraine's energy sector in December 2016.

Russian-Backed Cyber Threat Activity

UC RIVERSIDE Office of Emergency Management

Even as the administration received **positive** marks for its **collaboration** with **industry** to mitigate the Log4j software **vulnerability**, all eyes are on Ukraine. With a Russian invasion increasingly likely, hackers deleted **data** and temporarily **disabled** websites of Ukrainian government agencies in mid-January. Microsoft also **identified** destructive **malware** in Ukrainian government and corporate **systems**. The malware **resembles** that used in Russia's 2017 NotPetya attack, which cost companies around the world $10 billion. Following the most recent cyberattacks, Washington and NATO **provided** information to help Kyiv counter malicious cyber operations, building on December's **reported deployment** of U.S. and UK cyber experts to Ukraine.

Meanwhile, Washington and its **allies** are **warning** critical **infrastructure** operators that Russia may **launch** disruptive attacks against the West. The Cybersecurity and Infrastructure Security Agency issued **tailored guidance** on best practices to mitigate threats to critical systems and a technical **advisory** on common Russian tactics.

Why Does This Matter To The UC/UCR?

UC RIVERSIDE Office of Emergency Management

- There is an increasing concern that cyber-attacks targeting Operational Technology (OT) could impact UC/UCR.
- Universities are not expected to be a direct target of a cyberattack, however, there is heightened concern around this type of attack because universities often have a significant footprint of industrial control systems.
- There is also a concern that even if the UC campuses are not directly targeted or impacted from an attack that these attacks will target power, water and other utilities that the campuses rely upon (EX: local government critical infrastructure).
- UCOP has stated they will put together a threat brief for OT groups across UC system to share this information with those that own/operate these types of systems.

QUESTION: Do all UC campuses have an equal chance of cyber attack or is there anything at UCR that would raise its profile or probability of attack?

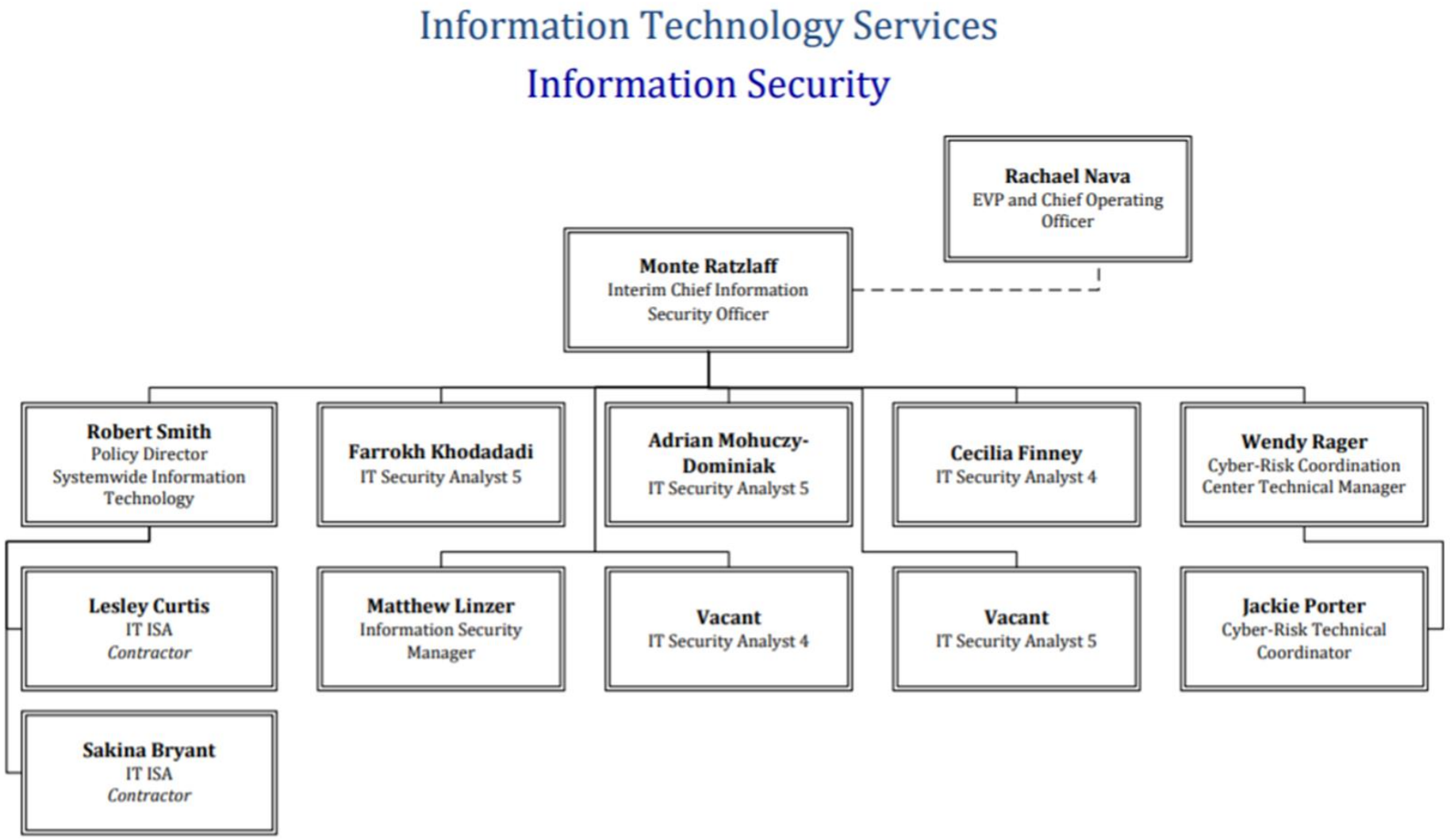
DEFINITIONS:

Information Technology (IT): Computing and/or communications hardware and/or software components and related resources that can collect, store, process, maintain, share, transmit, or dispose of data. IT components include computers and associated peripheral devices, computer operating systems, utility/support software, and communications hardware and software.

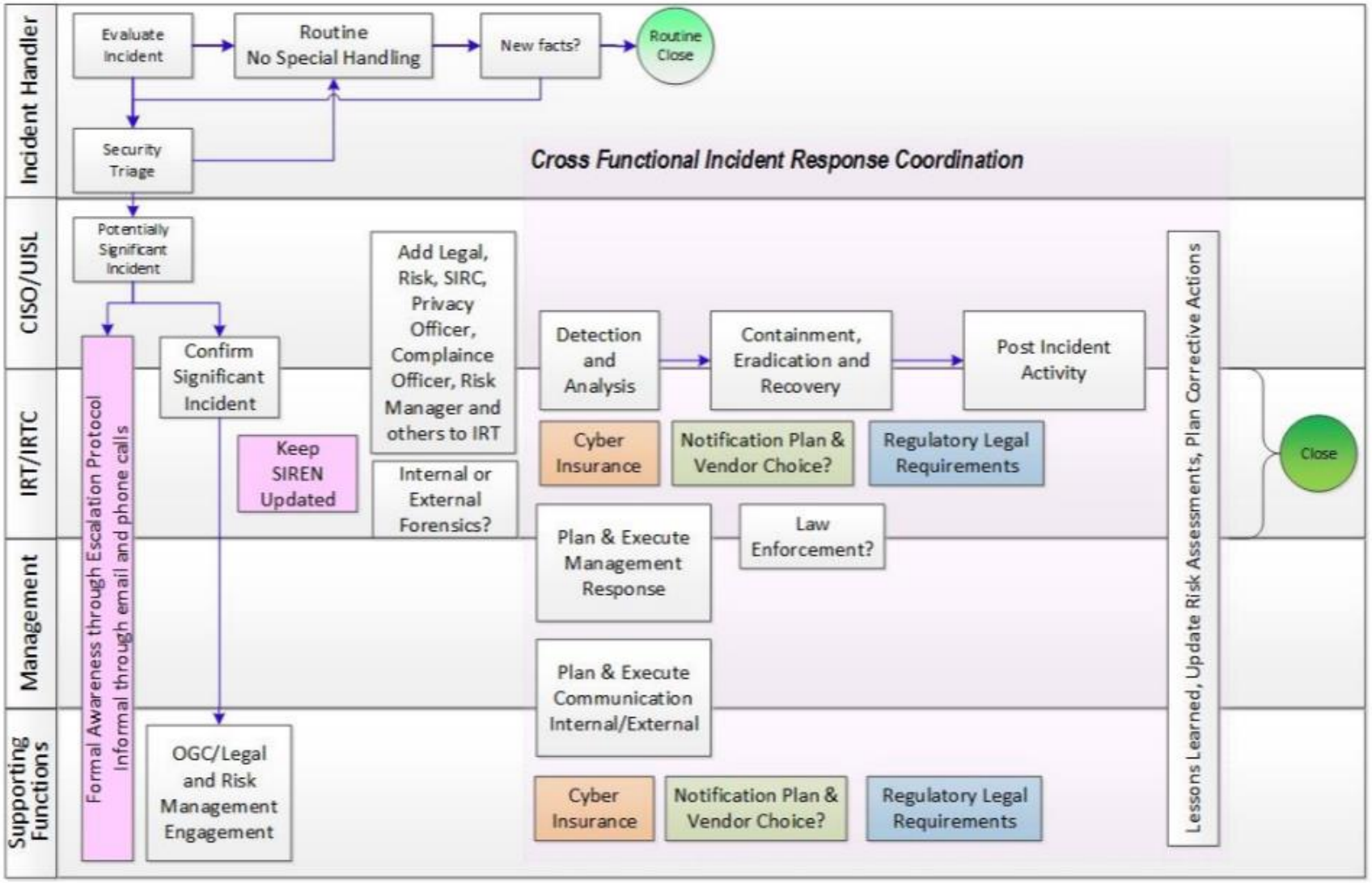
Operational Technology (OT): Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.

Industrial Control System (ICS): An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.

UCOP: ITS Information Security



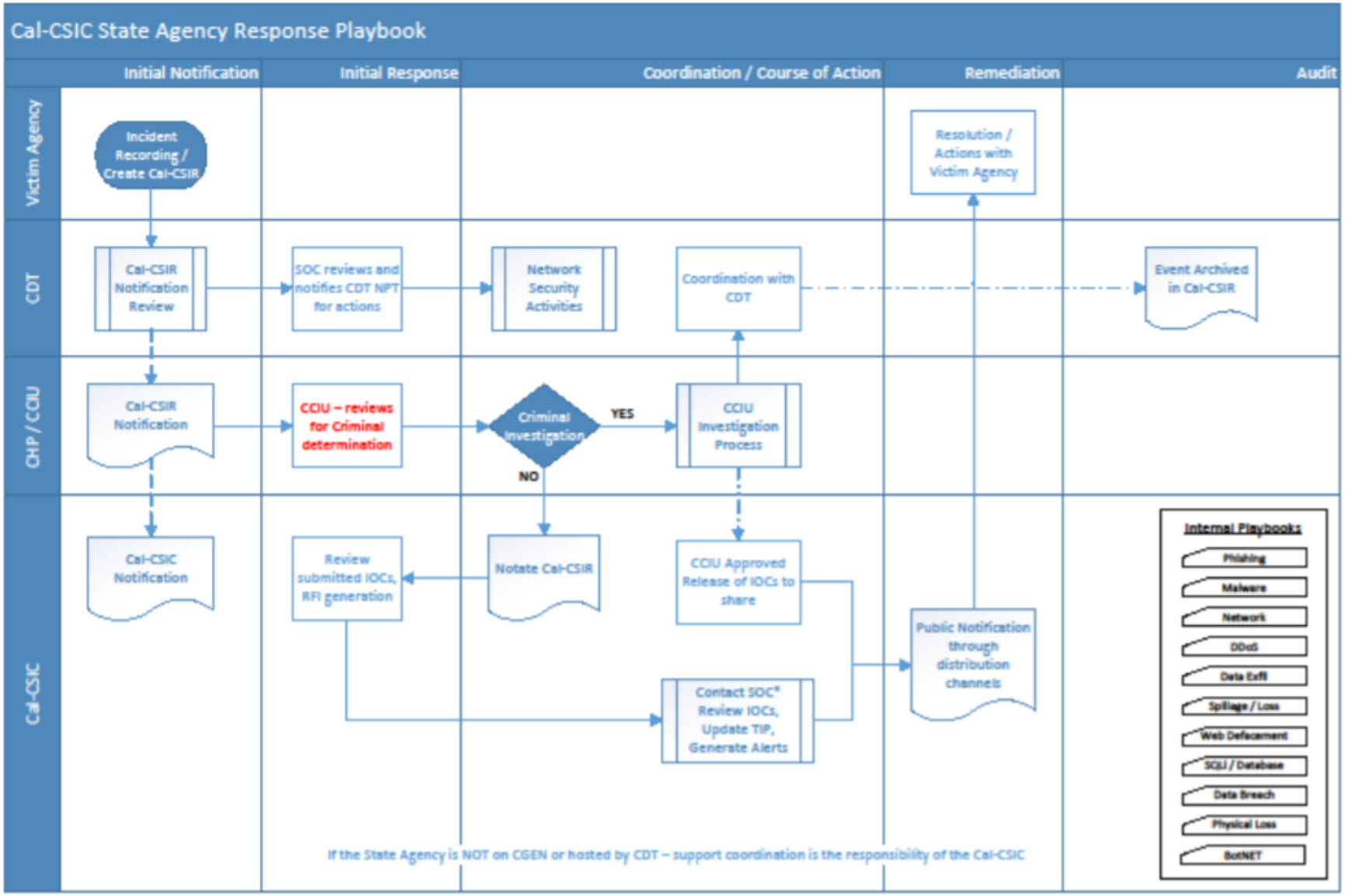
UCOP: Cyber Framework



The primary focus of this Standard is to provide assistance to Locations and Units as they develop their Information Security Incident Response Plans. The secondary goal of this Standard is to guide Locations in developing their overall Information Security Incident Response Program.

Cal-OES & Cal-CSIC: Cyber Framework

UC RIVERSIDE Office of Emergency Management



UCOP: Incident Response

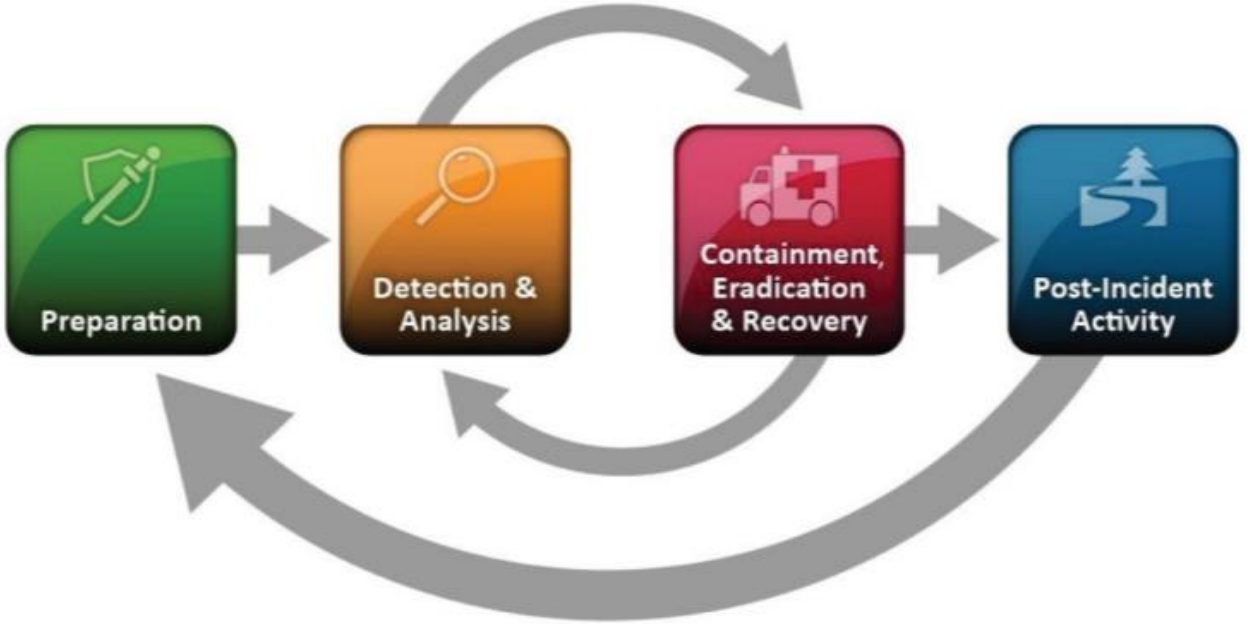


Figure 2

Incident Response Program Life Cycle

This section describes the establishment of the overall Information Security Incident Response Program.

This section covers:

- Preparation.
- Detection and Event Analysis.
- Containment, Eradication and Recovery.
- Post-Incident Activity.

UCOP: Protection Level Classifications

UC RIVERSIDE Office of Emergency Management

Protection Level Classification	
Level	**Impact of disclosure or compromise**
P4 - High	Institutional Information and related IT Resources whose unauthorized disclosure or modification could result in significant fines, penalties, regulatory action, or civil or criminal violations. Statutory, regulatory and contract obligations are major drivers for this risk level. Other drivers include, but are not limited to, the risk of significant harm or impairment to UC students, patients, research subjects, employees, guests/program participants, UC reputation, the overall operation of the Location or essential services. (Statutory.)
P3 - Moderate	Institutional Information and related IT Resources whose unauthorized disclosure or modification could result in small to moderate fines, penalties or civil actions. Institutional Information of which unauthorized use, access, disclosure, acquisition, modification, loss or deletion could result in moderate damage to UC, its students, patients, research subjects, employees, community and/or reputation; could have a moderate impact on the privacy of a group; could result in moderate financial loss; or could require legal action. This classification level also includes lower risk items that, when combined, represent increased risk. (Proprietary.)
P2 - Low	Institutional Information and related IT Resources that may not be specifically protected by statute, regulations or other contractual obligations or mandates, but are generally not intended for public use or access. In addition, information of which unauthorized use, access, disclosure, acquisition, modification or loss could result in minor damage or small financial loss, or cause minor impact on the privacy of an individual or group. (Internal.)
P1 - Minimal	Public information or information intended to be readily obtainable by the public, but whose integrity is important and for which unauthorized modification is the primary protection concern. IT Resources for which the application of minimum security requirements is sufficient. (Public.)

Cal-OES & Cal-CSIC: Cyber Incident Matrix

UC RIVERSIDE Office of Emergency Management

California Cyber Incident Severity	Description	Level of Effort—Description of Actions
Level 0—Steady State	Unsubstantiated or inconsequential event.	Steady State, which includes routine watch and warning activities.
Level 1—Low	Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	Requires coordination among State Departments and SLTT governments due to minor to average levels and breadth of damage. Typically, this is primarily a recovery effort with minimal response requirements.
Level 2—Medium	May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	Requires coordination among Victim Departments, Victim Agencies, or SLTT governments due to minor to average levels and breadth of cyber related impact or damage. Typically, this is primarily a recovery effort.
Level 3—High	Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	Requires elevated coordination among State Departments, State Agencies, or SLTT governments due to moderate levels and breadth of damage. Potential involvement of FEMA and other federal agencies.
Level 4—Severe	Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.	Requires elevated coordination among State Departments, State Agencies, or SLTT governments due to moderate levels and breadth of cyber impact or damage. Involvement of Federal Partners if needed for incident.
Level 5—Emergency	Poses an imminent threat to the provision of wide-scale critical infrastructure services, State government security, or the lives of California citizens.	Due to its severity, size, location, actual or potential impact on public health, welfare, or infrastructure, the cyber incident requires an extreme amount of State assistance for incident response and recovery efforts, for which the capabilities to support do not exist at any level of State government. Involvement of Public-Private Partnerships if needed for incident.

UCOP: Roles and Responsibilities

UC RIVERSIDE Office of Emergency Management

6 Appendix A – Roles and Responsibilities

Role	Responsibility
Cyber-risk Responsible Executive (CRE)	Responsible for the appointment of the Lead Location Authority/Authorities (e.g., Campus LLA, Health LLA). Ensures that the Cyber Escalation Protocol is followed.
Lead Location Authority (LLA)	Responsible for the overall development, execution, improvement and maintenance of the Information Security Incident Response Plan and Program. Determines when to convene the IRT, appoints the IRTC and facilitates making the decision to notify affected parties.
IRT Coordinator (IRTC)	Responsible for assembling the Incident Response Team, capturing and documenting all the data pertinent to an Incident, communicating with appropriate parties, ensuring that the information is complete and reporting on Incident status both during and after the investigation.
Privacy Officer	Responsible for assessing privacy impacts and recommending what notification should occur, if any.
CISO	Responsible for assessing the impact of an Information Security Incident, the effectiveness of controls, the effectiveness of detection, the effectiveness of containment and recovery strategies and making recommendations for reducing/managing cyber risk.
Incident handlers	Responsible for containing the Incident, adjusting protective/detective tools and/or controls. Gathers and/or investigates technical details, documents the Incident investigation, determines root cause, obtains forensic evidence and preserves and analyzes evidence so that an Information Security Incident response can be brought to a conclusion.

Role	Responsibility
Legal Counsel - Location	The advisor on legal risks and obligations who serves as the liaison with OGC. Provides advice on the extent and form of all disclosures to law enforcement and the public. Makes determinations related to the scope and nature of investigations.
Risk Management and/or Risk Services	Responsible for assessing operational risks at the Location, implementing programs to reduce claims at the Location and filing cyber insurance claims.
Unit Information Security Lead	Responsible for ensuring a Unit has the technical controls, detection processes and response processes in place to address cyber security events and Incidents. See section 3 above. Supports IRT as required.
Unit Head	Responsible for ensuring that Unit resources and the Unit Information Security Lead support Incident response. In coordination with the IRTC, communicates with key stakeholders and sponsors or contracted parties.
Workforce Member	Every Workforce Member at UC has the responsibility to report immediately suspected or known unauthorized access of Institutional Information or IT Resources to the designated Unit Information Security Lead or the designated individual for their work area. This may be a local support person, an IT Help Desk, departmental management, compliance officer/department or similar function, as defined by the Location. Criminal acts, such as thefts or suspected criminal acts, must also be reported to campus police.

Contacts: Cal-CSIC

UC RIVERSIDE Office of Emergency Management

California Cybersecurity Integration Center (Cal-CSIC)

- **Mission:** The California Cybersecurity Integration Center's primary mission is to reduce the likelihood and severity of cyber incidents that could damage California's economy, its critical infrastructure, or public and private sector computer networks in our state.
- **Website:** www.caloes.ca.gov/cyber
- **Services:**
  - Threat Intelligence
  - Advisory
  - Incident response

On 31 August 2015, the Governor of California signed Executive Order B-34-15, creating the California Cybersecurity Integration Center (Cal-CSIC).

On 26 September 2018, the Governor of California approved Assembly Bill 2813, in support of California's statewide cybersecurity strategy.

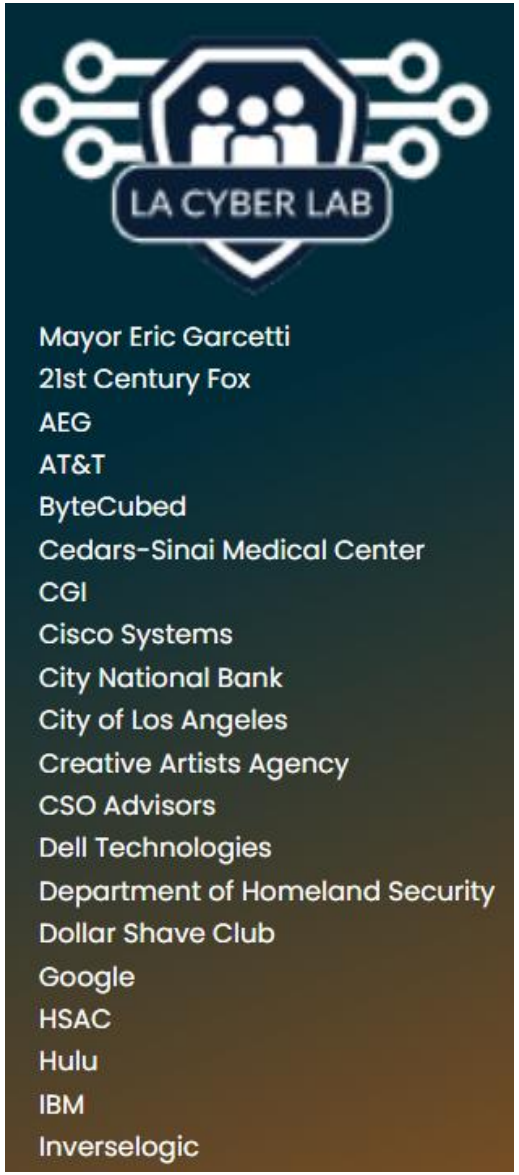
The passing of AB2813 added Section 8586.5 to the California Government Code which further defines the structure and the mission of the Cal-CSIC:

The California Cybersecurity Integration Center shall serve as the central organizing hub of state government's cybersecurity activities and coordinate information sharing with local, state, and federal agencies, tribal governments, utilities and other service providers, academic institutions, and nongovernmental organizations.

Contacts: LA Cyber Lab

LA Cyber Lab

- **Mission:** The mission of the LA Cyber Lab is to provide the greater Los Angeles business community and local government organizations with greater cybersecurity awareness and access to trained and capable workforce.
- **Website:** https://www.lacyberlab.org/
- **Services:**
  - Threat Intelligence
  - Advisory



Contacts: JRIC

Joint Regional Intelligence Center (JRIC)

- **Mission**: Protect the people, infrastructure, and economy of the Central District of California from terrorism and criminal activity by analyzing and disseminating threat intelligence to local, state, tribal, and federal partners.
- **Website**: www.jric.org
- **Services:**
  - Threat Intelligence
  - Advisory
  - Local, State & Federal Law Enforcement Liaison

- **The Joint Regional Intelligence Center (JRIC) was established in 2006 as a cooperative effort between federal, state, and local law enforcement and public safety agencies to centralize the intake, analysis, synthesis, and appropriate dissemination of terrorism-related threat intelligence for the greater Los Angeles region.**

- **The JRIC also serves as the Regional Threat Assessment Center (RTAC) for the Central District of California as part of the California State Threat Assessment System (STAS).**

Contacts: California State Guard (CSG)

California State Guard (CSG)

- **Mission**: The California State Guard (CSG) is a force that protects California and its citizens from natural and man-made disasters, including wildfires, floods, earthquakes, and pandemics. It was formed to provide California with a trained and organized force in the event of a state emergency.
- **Website**: https://stateguard.cmd.ca.gov/public/
- **Services:**
  - Exercise / response planning
  - Free penetration testing

Contacts: Cyber Resilience Center (CRC)

Port of Los Angeles Cyber Resilience Center (CRC)

- **Mission**: The Port of Los Angeles Cyber Resilience Center (CRC) is a community cyber defense solution created to improve the cybersecurity readiness of the Port and enhance its threat-sharing and recovery capabilities among supply chain stakeholders. **Website**: https://www.portoflosangeles.org/
- **Services:**
  - Threat-sharing & recovery capabilities
  - Become a supply chain stakeholder

Port Of Los Angeles Launches First-of-its-kind Cyber Resilience Center

- **Enables Port Stakeholders to Enhance Cyber Threat Information Sharing and Recovery Measures to Reduce Risk of Disruption Flow.**
- **The center will help protect North America's largest seaport from cyber threats and serve as a hub for the Port to receive, analyze and share cybersecurity information among its stakeholders.**

REFERENCES

- Russia has been at war with Ukraine for years -- in cyberspace
- White House, EPA release 100-day cybersecurity plan for water utility operators
- How The NSA, NSF And Academia Are Working To Prevent Future Cyberattacks
- Preparing For Inevitable Cyber Surprise
- 'Hacktivist' Cyber Disruption Could Spread to Russia, Experts Believe
- Wilson Center: Focus Ukraine
- Russian Troop Movements and Tensions Along the Ukrainian Border
- If Putin wins, it's not only Ukraine that loses
- The "Crisis Crossroads" page highlights analysis on the situation in Ukraine
- Hybrid war & Ukraine
- The differences between Incident Response, Disaster Recovery, and Business Continuity
- Building A Business Case for Operational Technology Cybersecurity
- Conversation with a top Ukrainian cyber official: What we know, what we don't, what it means
- WhisperGate Malware Corrupts Computers in Ukraine
- Lawmaker Pushes for Disaster Declaration After Cyber Attacks
- Ukraine Continues to Face Cyber Espionage Attacks from Russian Hackers
- Over half of attacks are targeting finance, utilities & retailers
- Researchers break down WhisperGate wiper malware used in Ukraine website defacement
- Russia Has Carried Out 20-Years Of Cyber Attacks That Call For International Response
- Ukraine thinks Russia unlikely to invade 'for the next two weeks'

RESOURCES

- UCOP ITS Systemwide IT Policy UC Information Security Incident Response Standard
- Carnegie Mellon University Incident Response Procedure
- Mitigating Higher Ed Cyber Attacks
- Securing Higher Ed against cyberthreats: from an institutional risk to a national policy challenge
- A Systematic Review of Cybersecurity Risks in Higher Education
- Leaked text suggests possible US-Russia missile arrangement over Ukraine
- Cybersecurity Report 2021: In-Depth Analysis of Vulnerabilities Affecting Industrial Control Systems
- NATO written responses to Russian demands, leaked by El Pais
- Russian invasion of Ukraine could redefine cyber warfare
- Timeline: Ukraine's turbulent history since independence in 1991
- Case Studies: The early days of cyberattacks: the cases of Estonia, Georgia and Ukraine
- How Moscow, Washington, Kyiv, and Brussels are preparing for the possibility of war.
- Cyber Conflict Around the Globe
- Over half of attacks are targeting finance, utilities & retailers
- CISA: Rising Ransomware Threat To Operational Technology Assets
- NIST: Operational Technology Security
- Managing risks in Operational Technology systems
- The Ultimate Guide to Understanding Operational Technology Security
- GE: An Executive Guide to Cyber Security for Operational Technology
- White House Releases Memo on Cybersecurity at Federal Agencies