USAID
FROM THE AMERICAN PEOPLE

CROWDSTRIKE

POWER UTILITY DATA PROTECTION POLICIES AND PRACTICES

DREW BAGLEY, CIPP/E

VP & COUNSEL, PRIVACY & CYBER POLICY

USEA
United States Energy Association

- Data Protection Basics
- Protecting Utility Data
- Threats to Data Protection
- Best Practices

DATA PROTECTION

Integrity

Reliable data is vital for reliable energy

Availability

Data availability is critical for using data to provide electricity

Confidentiality

Protected power grid data is crucial to prevent disruption

CROWDSTRIKE

DATA IS EVERYWHERE

Customer

Employee

IT infrastructure

SCADA

SmartGrid/IoT devices

Other confidential data

(e.g. Trade Secrets, Intellectual Property, Supply Chain Mapping)

DIFFERENT ROLES HAVE DIFFERENT RESPONSIBILITIES

Data subject
The individual whose information is being collected and processed

Data controller
Entity determining the purposes and means of processing data from the data subject (i.e. collects the data)

Data processor
Organization processing data on behalf of the data controller

CROWDSTRIKE

DATA OBLIGATIONS ARE EVERYWHERE

- Adherence to non-disclosure agreements (e.g. with clients, customers, vendors)
- Adherence to contractual security and privacy obligations
- Adherence to specific data protection and privacy regulations, such as those for:
  - Personal data/personally identifiable information
  - Protected health information
  - Financial data
  - National security data
- Need to protect proprietary data from being misused
- Obligations to update your register of processing activities
- Ability to comply with other obligations like E-Discovery

CYBERSECURITY IS KEY TO DATA PROTECTION

- The EU's General Data Protection Regulation requires organizations to implement "appropriate technical and organizational measures to ensure a level of security appropriate to the risk."
  - GDPR Art. 32(1)

- Under the California Consumer Privacy Act, organizations have a "duty to implement and maintain reasonable security procedures and practices."
  - CCPA § 1798.150

- The Australian Privacy Principles require "reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure"
- - APP 11.1

CRITICAL INFRASTRUCTURE CYBERSECURITY REQUIREMENTS

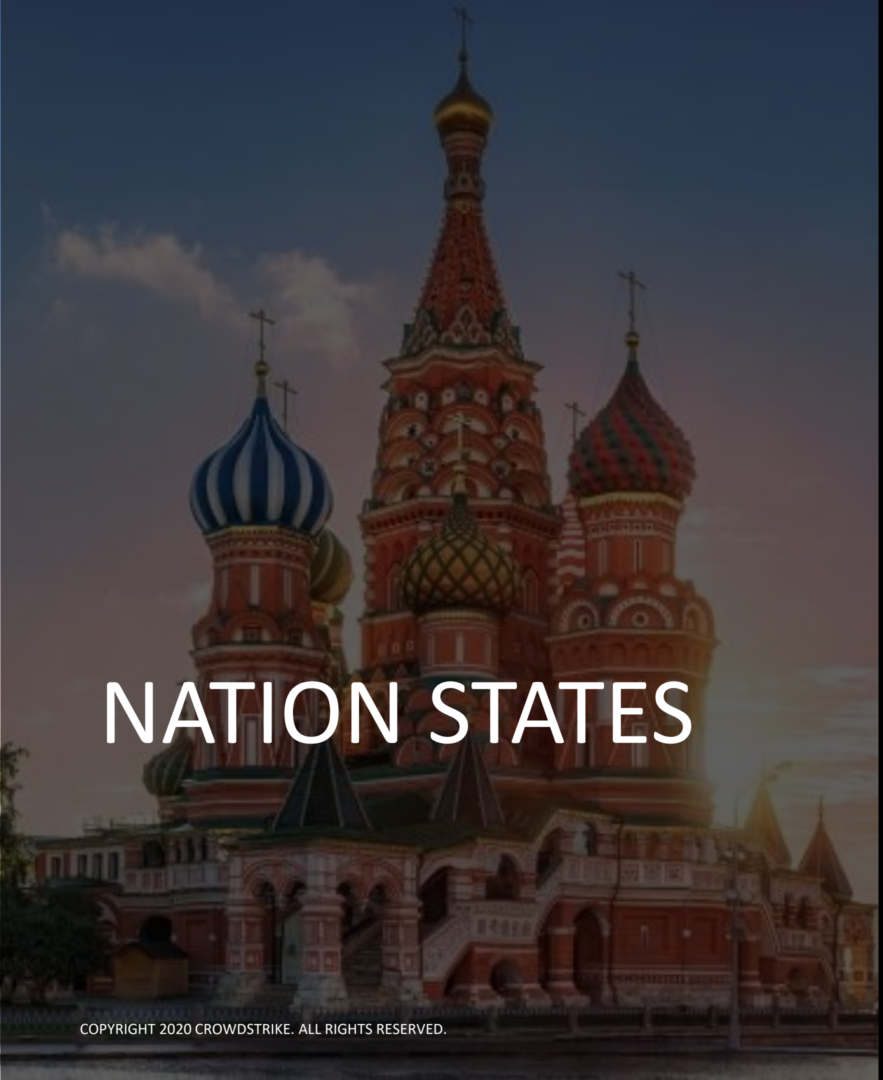
- Saudi Arabia Essential Cybersecurity Controls 2018
- European Union Network and Information Systems (NIS) Directive
- North American Electric Reliability Corporation’s (NERC) Critical Infrastructure Protection (CIP) cyber security reliability standards

BREACH NOTIFICATION IS GOING GLOBAL

Country	Name of Law	Sector/Data Type	Reporting Requirement
United States (federal)	The Health Insurance Portability and Accountability Act (“HIPAA”)	Protected health information	"Without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach"
United States (New York)	NYDFS Cybersecurity Requirements for Financial Services Companies	Financial entities	"As promptly as possible but in no event later than 72 hours"
European Union	General Data Protection Regulation ("GDPR")	Personal data	"Without undue delay and where feasible, not later than 72 hours after having become aware"
Canada	PIPEDA	Personal information	As soon as feasible where there is a "real risk of significant harm"
Brazil	Brazilian General Data Protection Law ("LGPD")	Personal data	Must report within "a reasonable time period"
Australia	Notifiable Data Breaches Scheme	Personal information	If “likely to result in serious harm” then ”expeditiously” and, where possible, within 30 days

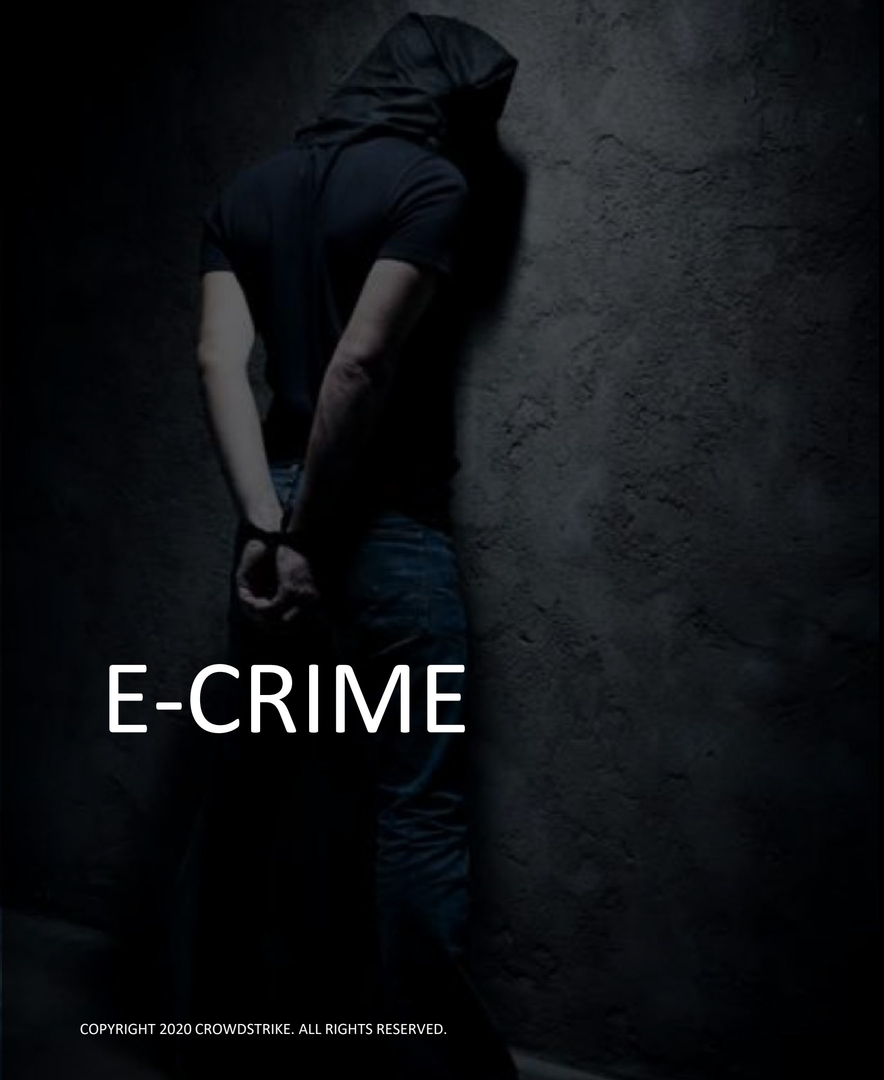
POWER UTILITY THREATSCAPE

- Credential harvesting
- Espionage
- Firmware corruption
- Data destruction
- Inhibit System Recovery
- Ransomware



NATION STATES

- Motivated by international events that drive intelligence requirements
- Programmatic collection conducted by professionals with a mission
- Potential impacts include
  - Disruption of electricity
  - Loss of business market advantage
  - Theft of IP
  - Disadvantageous deals/positions
  - Stock manipulation
  - Harvesting of industrial/political intelligence for influence ops



E-CRIME

- Motivation: financial gain, illicit transfers
- Cross sector targeting of small to large enterprises and bank accounts worldwide
- Tactics, Techniques, Procedures
  - Readily available remote access toolkits (RATs) providing the ability to snoop on victims
  - Use RATs to learn lexicon/hierarchy of victim organization, and then social engineering on a target with aim to transfer funds
  - Can use digital data to commit physical crimes (e.g. know when a residence or office is occupied)

HACKTIVISTS

- Motivation varies
- Impact
  - Disruption
  - Embarrassment
  - Destruction
- Tactics, Techniques, Procedures
  - Web Defacement
  - DDoS
  - Doxing
- Indications/Warnings
  - Hacktivism can occur at anytime, anywhere, for any reason

ASSUME YOU’RE A TARGET

Do you know the **data flows** and storage locations for all your **regulated** or **sensitive information**?

Do you know your **supply chain**?

Do you have appropriate **technical and organizational safeguards** in place?

STAY VIGILANT

- ✦Follow common data protection frameworks
  - ✦Transparency, purpose limitation, accuracy, storage limitation, integrity, confidentiality
- ✦Scrutinize the source/developer/legitimacy of software, hardware before connecting
- ✦Use two factor authentication
- ✦Use endpoint security that evolves in real-time as threats evolve
- ✦Be aware that IoT/SmartGrids are attractive for lateral movement, botnets, remote access, espionage, and destruction of infrastructure
- ✦Existing ICS certification models do not account for the realities of security
  - ✦ICS manufacturers can currently adopt “certified” AV, never update it, and not really be protected from modern threats (e.g. ransomware, malwareless attacks)

CROWDSTRIKE

THANK YOU

PRIVACY@CROWDSTRIKE.COM