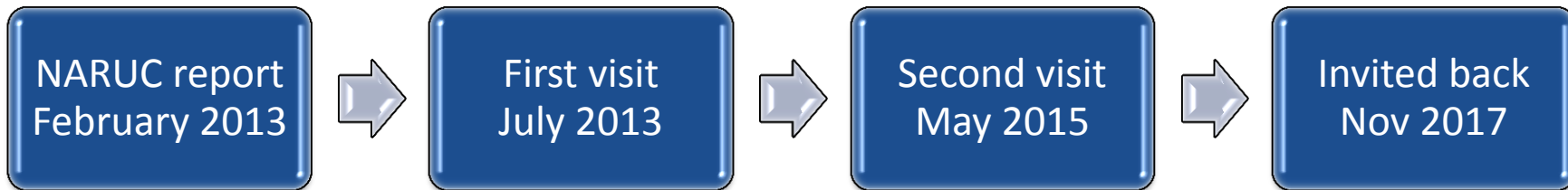


11/7/17



Cybersecurity and state regulators



“This document also proposes that **States engage strategically with cybersecurity** to enable and support a thoughtful, risk-based approach that encourages prudent investments by infrastructure operators.”



Cyber continues to be in the headlines

WannaCry

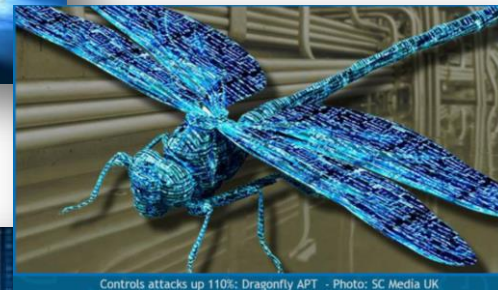
NotPetya

Crash
Override

DragonFly
2.0

Equifax

Deloitte

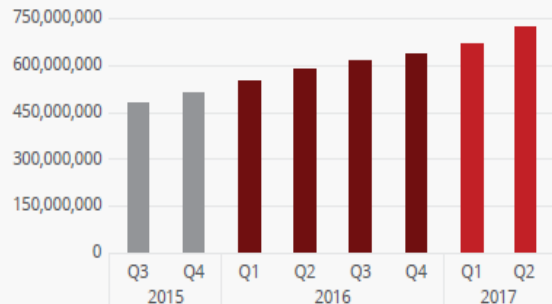


Controls attacks up 110%: Dragonfly APT - Photo: SC Media UK



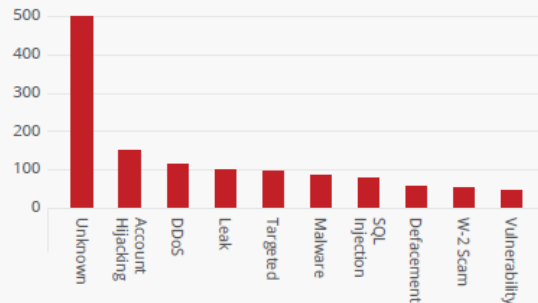
Not slowing down

Total malware



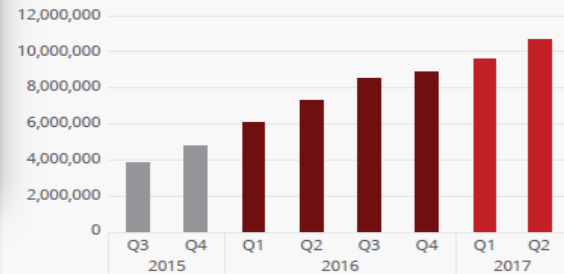
Source: McAfee Labs, 2017.

Top 10 attack vectors in 2016-2017
(Number of publicly disclosed incidents)



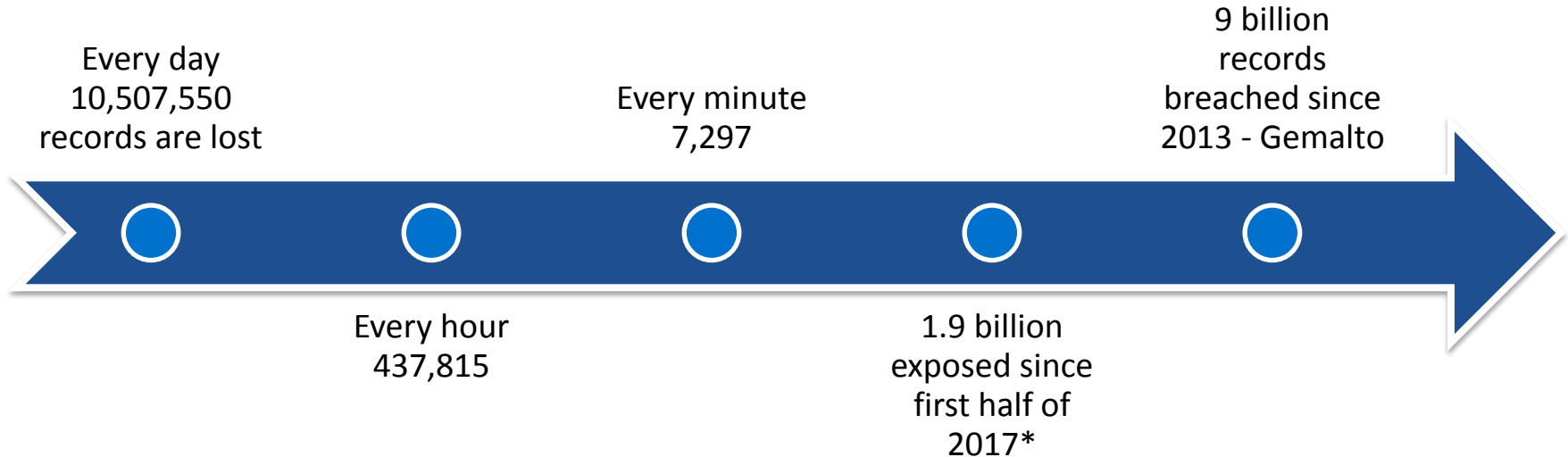
Source: McAfee Labs, 2017.

Total ransomware



Source: McAfee Labs, 2017.

Data breach context



* Not counting Equifax

Level set



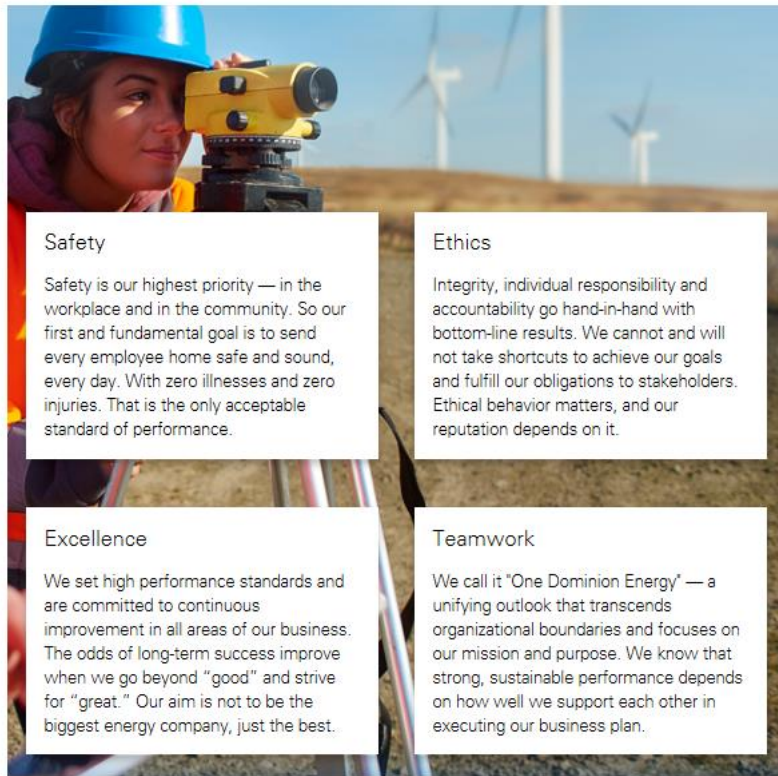
Mission and values

Our Mission

Serve our **customers** safely & reliably; Strengthen our **communities**; Minimize **environmental** impacts; Reward our **shareholders**; & Live our **values**.

Values & Commitments

Our Values



Safety

Safety is our highest priority — in the workplace and in the community. So our first and fundamental goal is to send every employee home safe and sound, every day. With zero illnesses and zero injuries. That is the only acceptable standard of performance.

Ethics

Integrity, individual responsibility and accountability go hand-in-hand with bottom-line results. We cannot and will not take shortcuts to achieve our goals and fulfill our obligations to stakeholders. Ethical behavior matters, and our reputation depends on it.

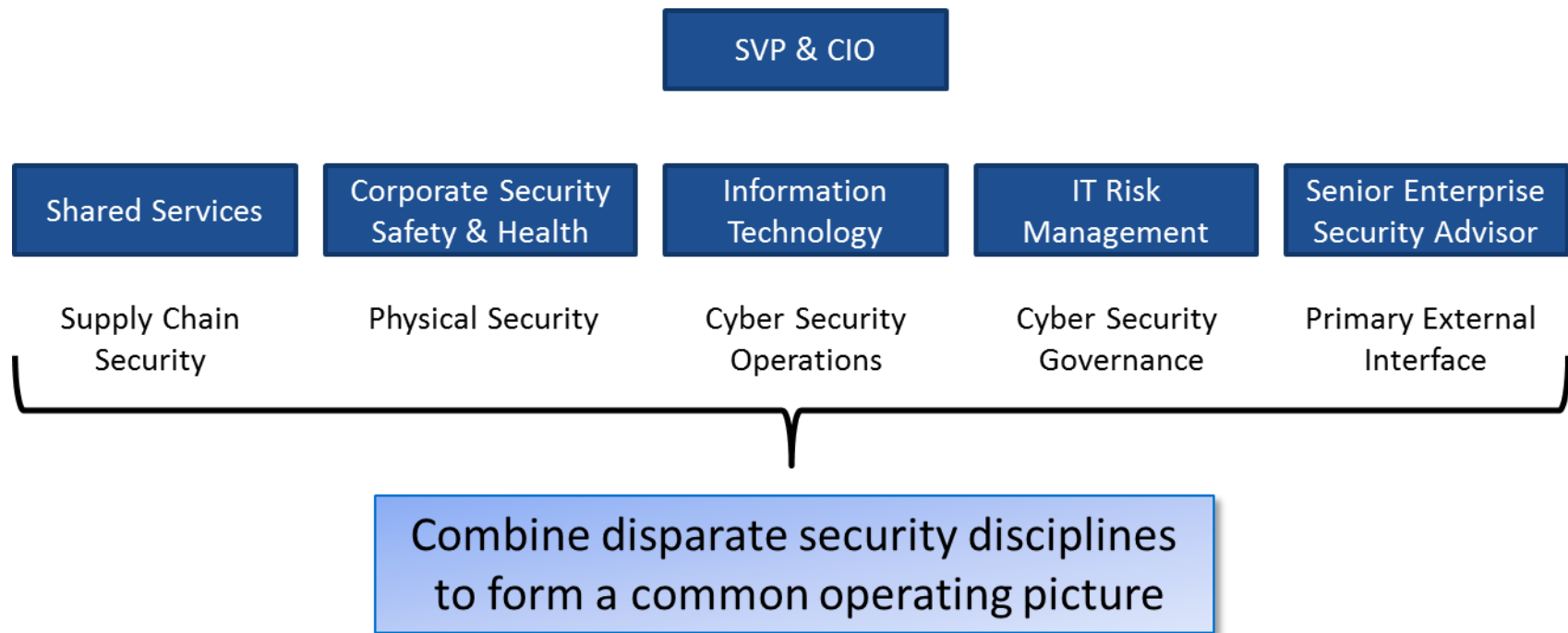
Excellence

We set high performance standards and are committed to continuous improvement in all areas of our business. The odds of long-term success improve when we go beyond “good” and strive for “great.” Our aim is not to be the biggest energy company, just the best.

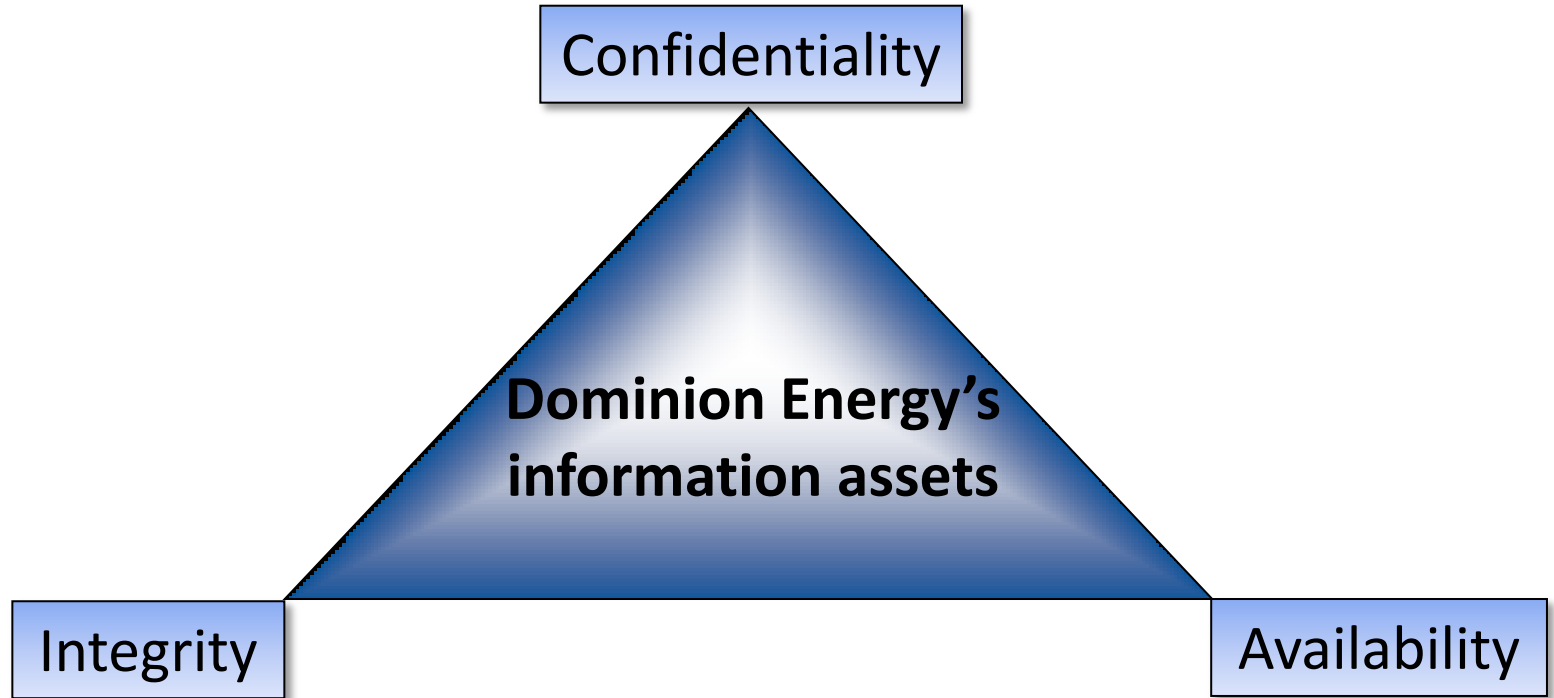
Teamwork

We call it “One Dominion Energy” — a unifying outlook that transcends organizational boundaries and focuses on our mission and purpose. We know that strong, sustainable performance depends on how well we support each other in executing our business plan.

Security oversight and coordination



Protect and ensure



Cybersecurity before merger

Awareness and Training

Monthly awareness , access to classified cyber information, employee training

Prevention

- Access Controls
- Email filtering
- Internet filtering
- Firewalls
- External assessments
- Development
- Network isolation

Detection

- Virus scans
- Intrusion detection
- SIEM-log monitoring
- Advanced threat detection
- Intelligence

Mitigation

- Review alerts
- Patch
- Manage vulnerabilities
- Disable defaults
- Forensics
- Incident response

Policies

Communication, training, compliance

Additional security measures

Third party risk management

Background checks for privileged users, contractors or vendors with unescorted access

New training

- Protecting information – data classifications 1 - 4
- General cybersecurity
- Phishing
- Privileged user

Monthly phishing simulations

24x7 Cybersecurity operations center (CSOC) monitoring

Third party risk management

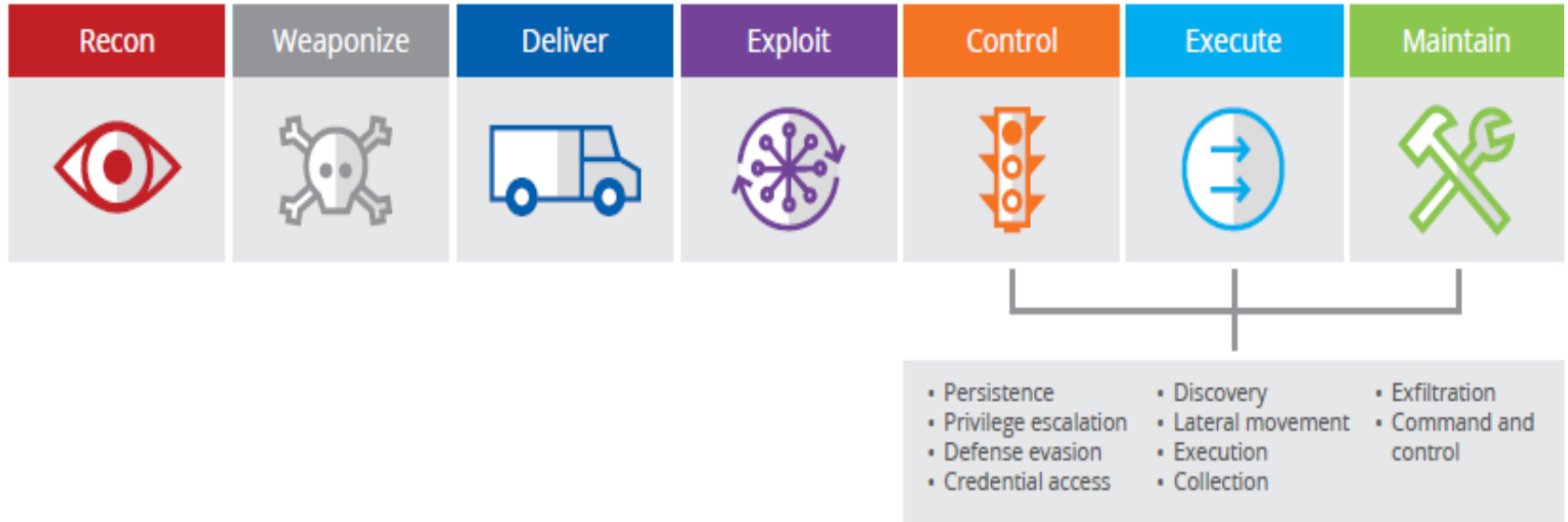


Reduce the risk of unauthorized disclosure of **Personally Identifiable Information (PII)**, including **Protected Health Information (PHI)**, stored and managed by a third party on behalf of Dominion Energy.


Connections and partnerships

Federal and Intelligence Community	States	Industry	Research and Development
Department of Energy (DOE)	Public Utility Commissions	Edison Electric Institute (EEI)	Defense Advanced Research Projects Agency (DARPA)
Department of Homeland Security (DHS)	National Association of Regulatory Utility Commissions (NARUC)	Interstate Natural Gas Association of America (INGAA)	Draper
Department of Defense (DOD)	State Governments	American Gas Association (AGA)	Idaho National Lab (INL)
Federal Bureau of Investigation (FBI)	State Police	Nuclear Energy Institute (NEI)	Pacific Northwest National Lab (PNNL)
National Security Agency (NSA)	National Guard	UNITE	DOE – Cybersecurity for Energy Delivery Systems (CEDS)
Transportation Security Administration (TSA)	Virginia Cyber Security Partnership	Electricity Sector Coordinating Council (ESCC)	
Department of Transportation (DOT)		Oil and Natural Gas Sector Coordinating Council (ONGSCC)	
Federal Energy Regulatory Commission (FERC)		Electricity Information Sharing and Analysis Center (E-ISAC)	
North American Reliability Corporation (NERC)		Downstream Natural Gas Information Sharing and Analysis Center (DNG-ISAC)	

Interrupt the kill chain



Commitment to Cyber Security

**Dominion Energy**[®]

Home & Small Business Large Business Safety Community About Us

Safety

Electric Safety

Natural Gas Safety

Call Before You Dig

Contractors

First Responders

Public Safety

> Nuclear Safety Planning

> Right of Way Use

> Grid & Substation Security

> Scammers & Personal Safety

Cyber Security

Just for Kids


Report an Emergency

Cyber Security

We use an integrated set of protections to safeguard critical energy infrastructure, the continuity of our operations and the confidentiality, integrity and availability of data and systems – including those involving customer and investor information.

In addition, Dominion Energy employees receive periodic cyber security awareness training to complement job-specific training. We safeguard customer information on secure systems with restricted access. Multiple security controls help protect this information whenever we store or transmit it.

A continuous monitoring program and internal and external audits provide ongoing oversight of our operations. Dominion Energy cyber security experts regularly communicate with government agencies, law enforcement and intelligence organizations and industry peers to assess threats and align the company's security posture with regulatory requirements and evolving digital technologies.



“Regulators are already doing significant work....., but the key to successful cybersecurity may prove to be **the development of a partnership between public and private actors to create a cybersecurity structure and culture that can meet the current needs while also being flexible enough to meet the ever-evolving threat.”**