

It's About the People

A Culture of Cybersecurity

Employees are the hidden key to cyber resilience

MICHAEL A. ECHOLS

- Max Cybersecurity LLC
- CEO International Association of Certified ISAOs

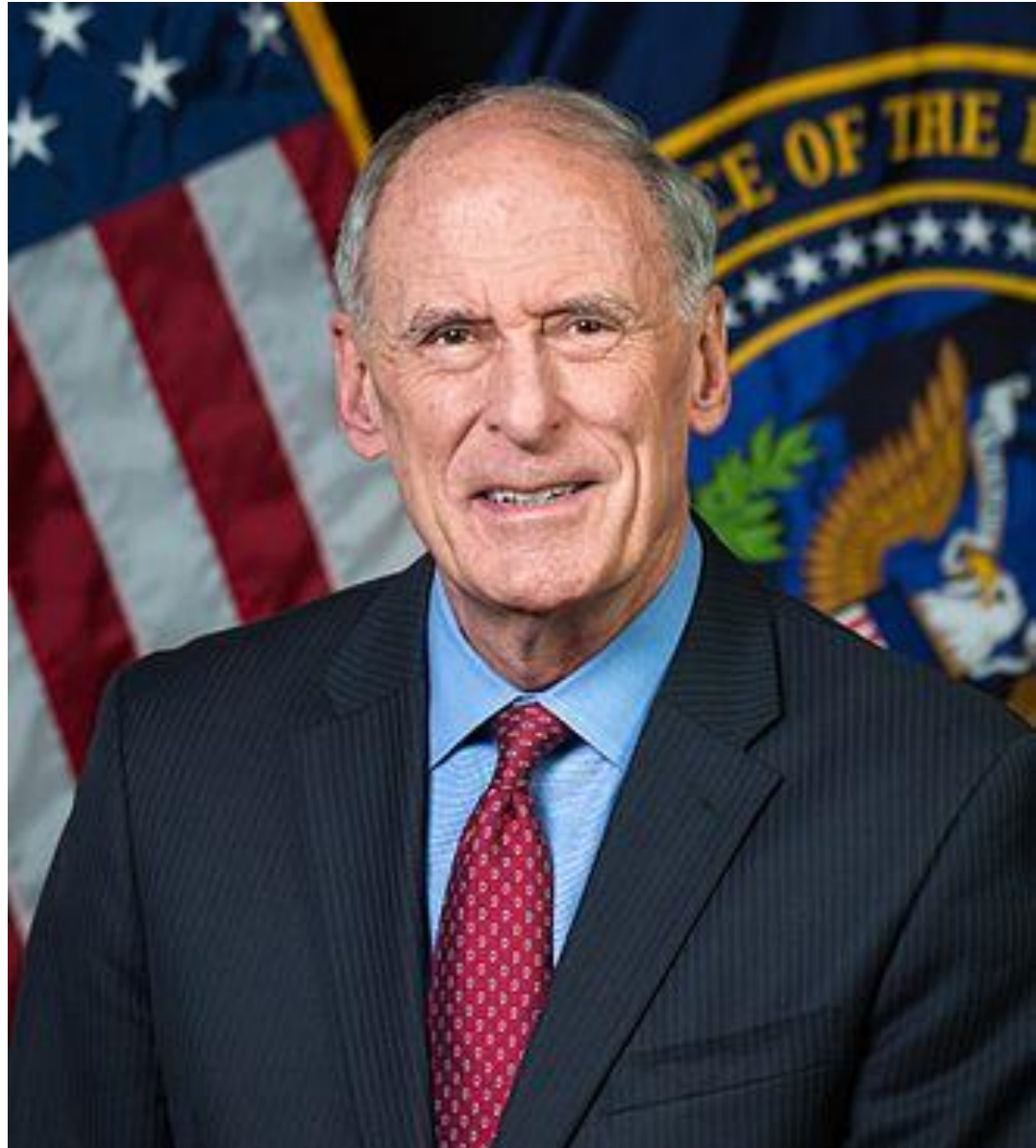
Clear and Present Danger

- Cyber attacks and security breaches are **increasing** in frequency and sophistication, with discovery after the fact, **if at all**.
- Targeting of organizations and individuals with malware and anonymization techniques that can **evade current controls**.
- Current perimeter-intrusion detection, signature-based malware, and anti-virus solutions are providing **little defense** and are rapidly becoming obsolete—Use encryption technology to avoid detection.
- Criminals are **leveraging innovation** and moving at a pace and security vendors cannot possibly match.

National Security Issue

Growing Concerns for Control Systems

"The system was blinking red. Here we are nearly two decades later and I'm here to say the warning lights are blinking red again"



Partnership Issue

"Between government and the private sector, we have the data needed to disrupt, prevent and mitigate cyberattacks. But we aren't sharing fast enough or collaborating deeply enough to keep cyberattacks from spreading or to prevent them in the first place."



Kirstjen Nielsen:
Secretary, Department of
Homeland Security

Concerns for Control Systems

Testimony to House Select Intelligence Committee –

“There shouldn’t be any doubt in our minds that there are nation-states and groups out there that have the capability to enter industrial control systems and to shut down [and] forestall our ability to operate our basic infrastructure.”

“All of that leads me to believe it is only a matter of the ‘when,’ not the ‘if’ that we are going to see something dramatic.”



Former NSA Director,
Michael Rogers

Democracy is under threat!

- Elections
- Evidence - Chain of custody
- Deep Fake Videos
- Politics



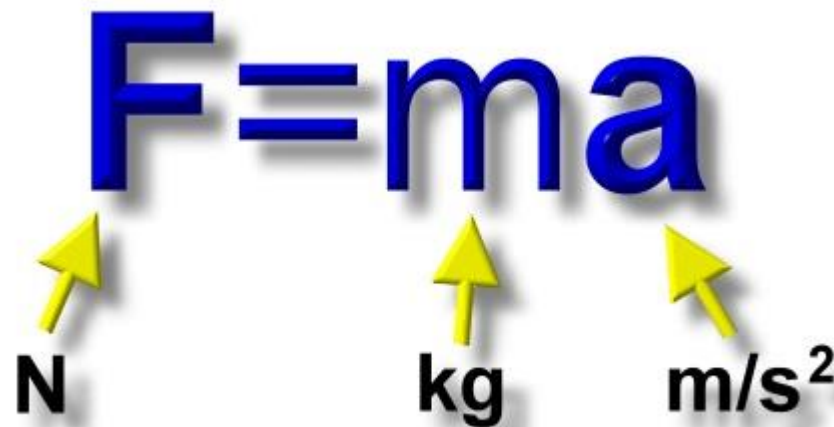
GOVERNMENT HACKINGS



Things are so bad the Government's energy is centered on protecting itself and critical infrastructure.

FORCE

The net **force** on an object is equal to the **mass** of the object multiplied by the **acceleration** of the object.

$$F = ma$$


The diagram illustrates the units for the variables in the equation $F = ma$. A yellow arrow points from the unit **N** (Newtons) to the variable **F**. Another yellow arrow points from the unit **kg** (kilograms) to the variable **m**. A third yellow arrow points from the unit **m/s²** (meters per second squared) to the variable **a**.

Cybersecurity

A man in a dark suit and tie is holding a glowing blue sphere in his right hand. In the background, a circular diagram with a central blue sphere is overlaid. The central sphere is labeled 'BUSINESS STRATEGY'. Surrounding it are eight smaller blue spheres, each containing a white icon and a label: 'Goals', 'Market', 'Vision', 'Risk', 'Network', 'Innovation', 'Value', and 'Growth'. The background is a blurred office interior with rows of chairs.



Source: Mario Morales, IDC

By 2020, the Internet of Things will have achieved "critical mass". Linking enormous intelligence in the cloud to billions of mobile devices and having extremely inexpensive sensors and tags embedded in and on everything, will deliver an enormous amount of new value to almost every human being. The full benefits—in terms of health, safety and convenience—will be enormous.

Straight Forward Formula

The Path Forward

Today

- Many unknown vulnerabilities
- Incidents spread at network speed and defenses are manual
- Many attacks are undetected
- Independently defended systems
- Inconsistent security policies
- Users do not follow best practices
- Attacks increasing in number and virulence

Future

- Baked in security = fewer vulnerabilities
- Near real-time response with more automated defenses
- Many attacks, but less impact
- Information sharing and increasingly collaborative defenses
- Consistent security practices
- Unauthorized activity quickly identified
- Ability to learn and adapt defenses in near-real time

Cybersecurity



CYBER HYGIENE
PRACTICES



NETWORK
SEGMENTATION

User Name:
Password:

UNRESTRICTED
USER ACCOUNTS



SERVER
DISCIPLINE



TWO-FACTOR
AUTHENTICATION



NETWORK
FLOW CAPTURE

Culture Shift

USER RISK LANDSCAPE

76% of Data Breaches Involved Stolen or Exploited User Accounts



Business Users

84% of insider-based breaches involve users with no admin rights



IT Users

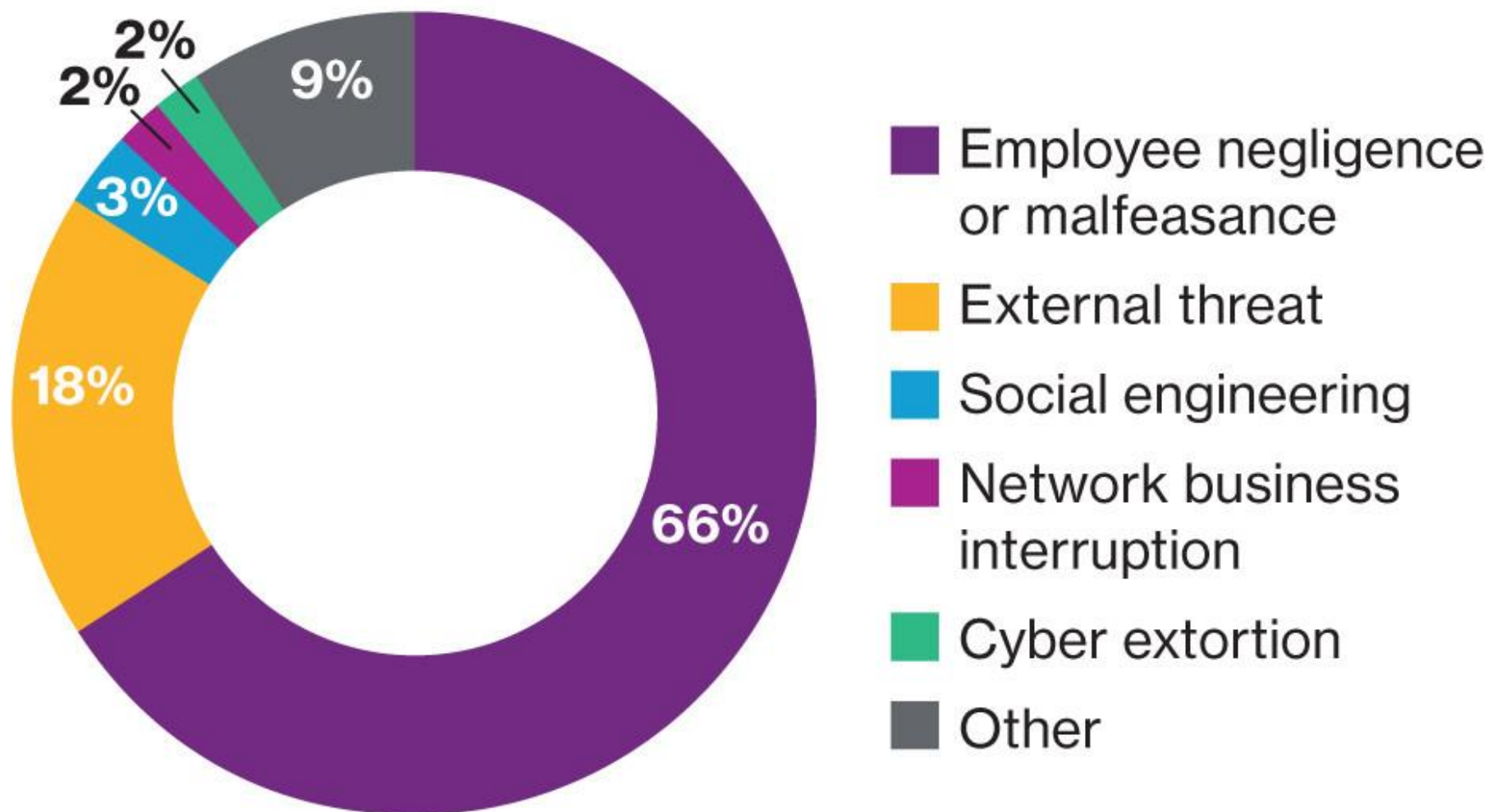
62% of admin-caused breaches are due to human error



Contractors

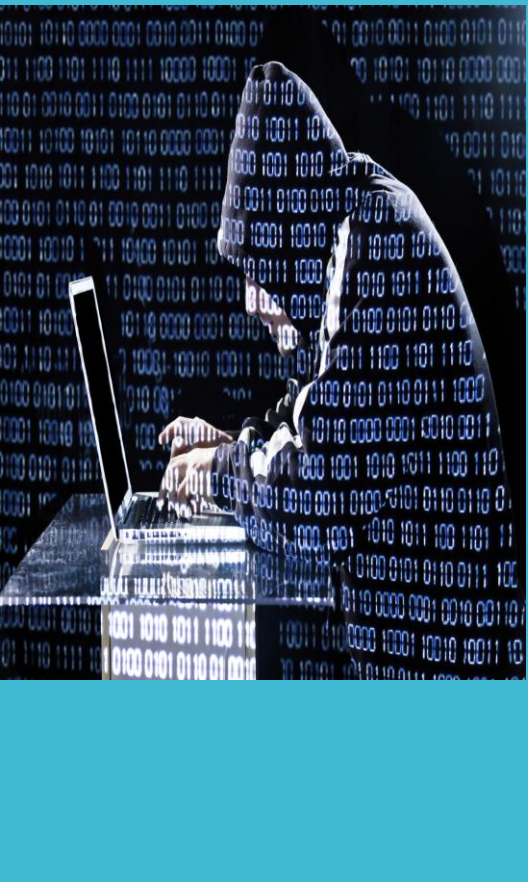
Breaches involving contractors have **significantly higher** data loss and severity

Percentage of claims by breach



Source: Willis Towers Watson cyber insurance claims data

Top Cyber Threat Attack Vectors



- **Spear Phishing / Watering Hole**
 - Organization email, personal webmail
- **Web Browsers**
 - Vulnerability exploitation (Adobe, Flash, Java)
 - Application patching
- **Web Servers**
 - Application and system patching
- **Remote Access**
 - Single factor (password-based)

Culture of Cybersecurity



“It is therefore up to security professionals to help their executives become more cybersecurity literate and thereby assist in framing security considerations as an integral part of any risk/opportunity discussion, as well as a wider enterprise risk management strategy.”

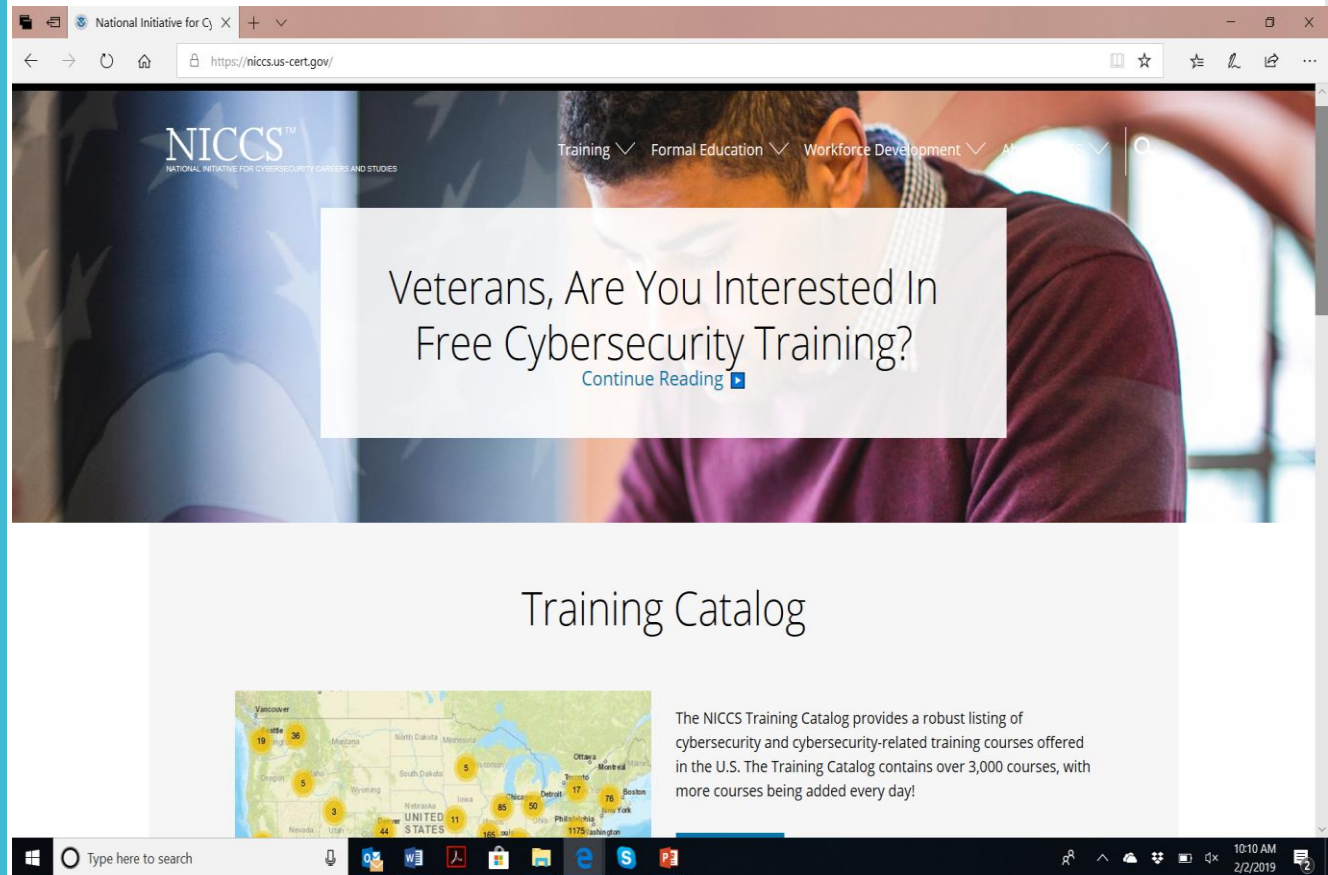
What are the expectations for cyber literacy?

Cyber Education

Resources for everyone – employees, employers, students, educators, parents, policy makers

- ✓ 5,000+ visitors per month
- ✓ 1,500+ training courses mapped to the National Cybersecurity Workforce Framework
- ✓ 100+ links to cybersecurity resources
- ✓ 15+ tools for managers
- ✓ 10+ monthly events
- ✓ 10+ links to customized job searches

Nation's One Stop Shop for Cybersecurity Careers & Studies!



<https://niccs.us-cert.gov/>

National Initiative for Cybersecurity Careers and Studies (NICCS)

The mission of NICE is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development

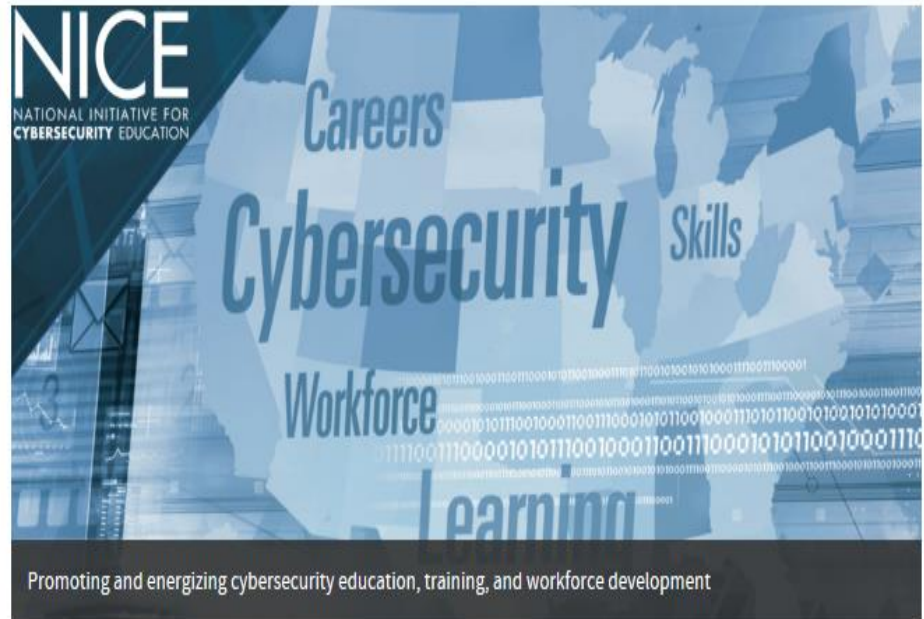
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE)

The mission of NICE is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development.



- About +
- News +
- Events +
- Resources +

CONNECT WITH US



<https://www.nist.gov/itl/applied-cybersecurity/nice>



QUESTIONS

Michael Echols

International Association of Certified ISAOs

www.certifiedisao.org

mechols@certifiedisao.org

mechols@maxcybersecurity.com

www.mikeechols.com

Connect on LinkedIn