David W. Loewy, PhD Chief Information Security Officer

SUNY **D**OWNSTATE Medical Center

Developing Your Organizations Ground Force in the Cyber Security War

David W. Loewy, PhD Chief Information Security Officer

George Jetson

Digital Index Operator

Lie in bed,

Turn off the lights

Count the number of little red lights staring back at you

And you think we don't live in a computer-centric world

Just a generation ago
The internet was little more than a link between a few university researchers

1st email 1971
In 2017 40 trillion emails were sent

1st website developed in 1991
In Dec 2017 1,805,260,010 were active

Email is the number one application

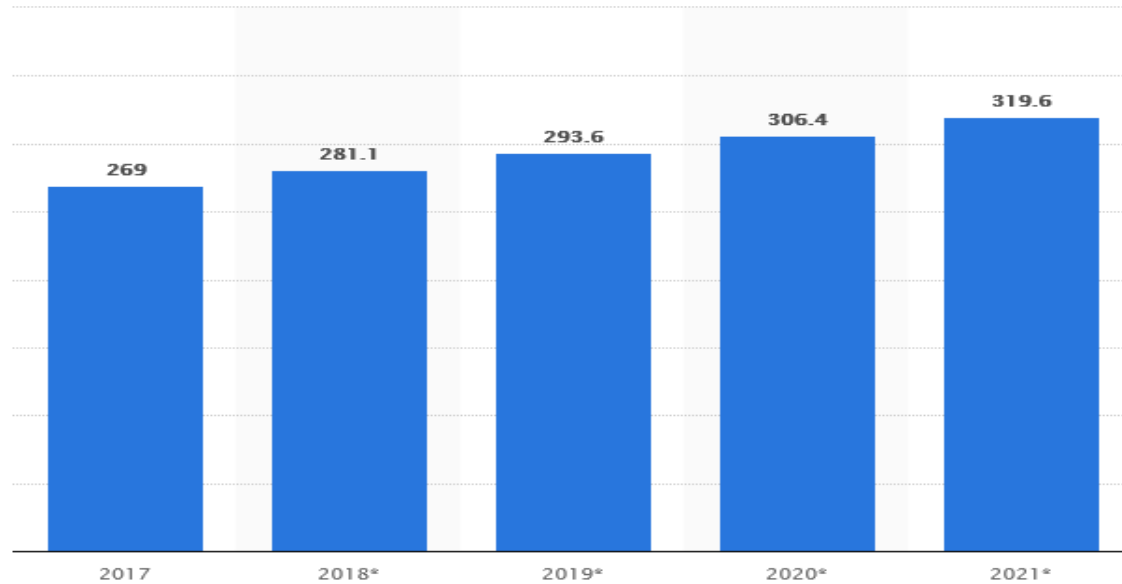used by business around the world

91% of known cyber attacks use email

as their preferred method of entry to systems and networks
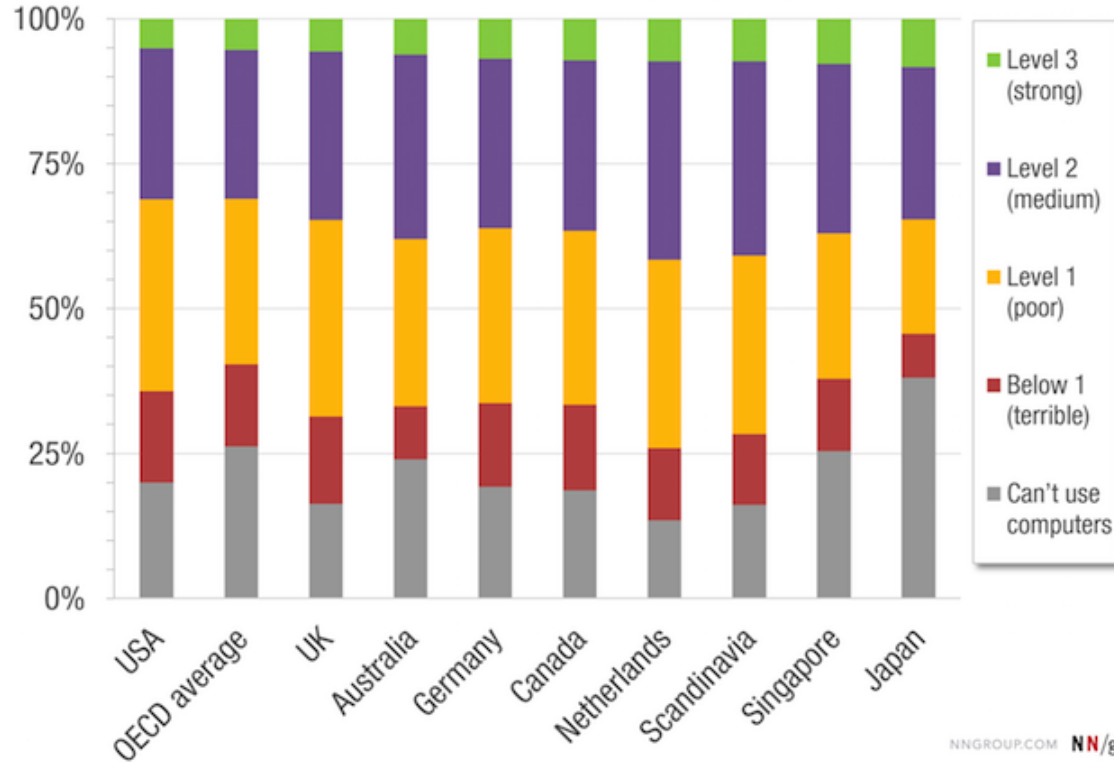
e-mails per day worldwide

Number of sent and received e-mails per day worldwide from 2017 to 2021. While roughly 269 billion emails were sent and received each day in 2017, the figure is expected to increase to almost 320 billion daily mails in 2021

Distribution of Computer Skills Among People Aged 16–65

Level 3: 5% of the population
This is the most skilled group of users.
At this level, participants were able to navigate
across pages and applications and use multiple tools to
reach a solution

Level 2: 26% of the population
Tasks at this level required some navigation across pages and applications in order to solve a
problem.

Cybersecurity
The cost and risks of cyber attacks are increasing

Cyber Threat Landscape

- Cybersecurity events and costs are increasing:
  - 79% of survey respondents detected a security incident in the past 12 months[1]
  - Average total cost of a data breach increased 23% over the past two years[2]
  - Average cost paid for each lost / stolen record increased 6%[1]

Industry Outlook

- Data breaches are expected to reach $2.1 trillion globally by 2019[3]
- 76% of survey respondents[1] were more concerned about cybersecurity threats than in previous 12 months:
  - Increase from 59% in 2014

Reputational Risk

- An IT security breach can have serious implications in how a company is perceived:
  - 46% of companies suffered damage to reputation & brand value due to a security breach[4]
  - 19% of companies suffered damage to reputation & brand value due to a third-party security breach or IT system failure[4]
- The risk of losing customer trust is significant and rising:
  - 82% of customers would consider leaving an institution that suffered a data breach[5]

The Threat Landscape

CRIMINALS

- **Impact:** Costly regulatory inquiries and penalties, consumer and shareholder lawsuits, loss of consumer confidence
- **Motivation:** Financial gain
- **2017 Outlook:** Cyber-extortion will continue to rise
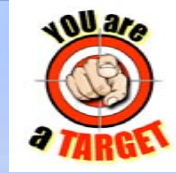
INSIDERS

- **Impact:** Competitive advantage, trade secret disclosure, operational disruption, brand and reputation
- **Motivation:** Personal advantage, monetary gain, professional revenge, patriotism
- **2017 Outlook:** More organizations will implement insider threat mitigation programs and processes
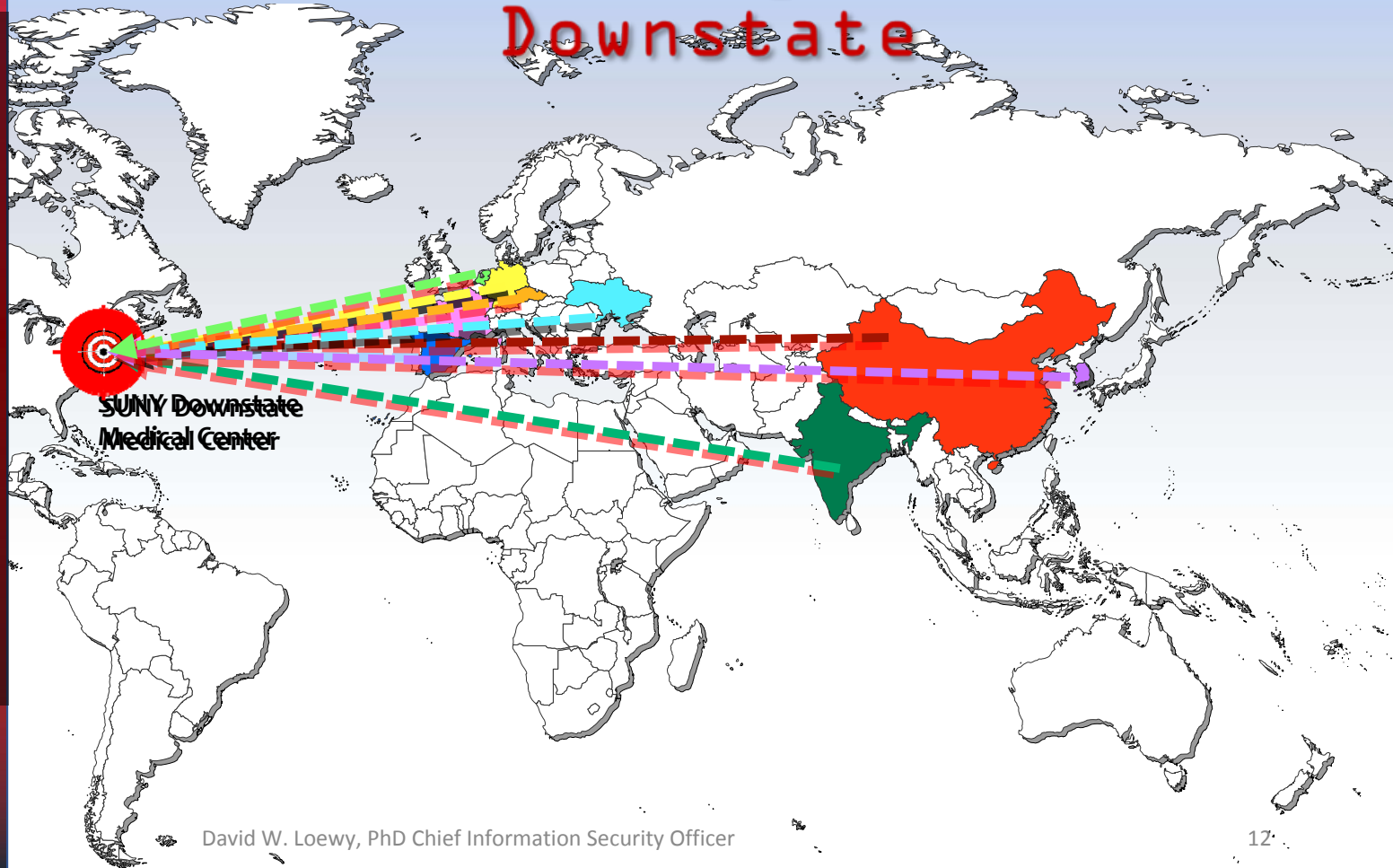
HACKTIVISTS

- **Impact:** Disruption of business activities, brand and reputation, loss of consumer confidence
- **Motivation:** Negatively impact reputation, drive attention to a cause, pressure for change
- **2017 Outlook:** Expected to escalate attack methods with high-profile data breaches

NATION STATES

- **Impact:** loss of competitive advantage, disruption to critical infrastructure
- **Motivation:** Economic, political, and/or military advantage
- **2017 Outlook:** Will continue to strengthen their defensive and offensive cyber skills

Amount of Cyber Attacks Every Four Hours

361	China	
112	Netherlands	
50	Ukraine	
17	Czech Republic	
16	Germany	
15	South Korea	
14	India	
14	Spain	
13	France	

YOU are a TARGET

Predominate Countries Attacking SUNY Downstate

SUNY Downstate Medical Center

David W. Loewy, PhD Chief Information Security Officer

12

- **The majority of cyber attacks are promulgated through emails**

- **20% of volatile emails can be caught and isolated through technology**

- **80% of emails are delivered and must be remediated by the receiving individual**

- **The current national ransomware epidemic infected and disabled computer systems via email**

Periodic Security Awareness

Periodic security awareness training develops essential competencies, new techniques and methods that are so essential in facing possible security issues.

Developing a Security Awareness Training program provides a significant level of maturity in incident response and help protect corporate resources;

Adopting a Security Awareness Training Program, security-related risk posture greatly increases. Security Awareness engages all members of the organizations workforce.

Awareness Campaign Activities

- Simulated Phishing
- Speakers
- Facility Wide Video Reminders
- Screensavers
- Newsletters
- Other Awareness Activities
  - Brownbag presentations
  - Helpdesk support
  - Institution Wide Email Notifications

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication

- Simulating phishing attacks to:
  - train employees,
  - quantify risk
  - harden workforce resiliency

National & World renown Speakers

o Head of FBI cyber security

o Neil Degrass Tyson (tentative)

o Sir Richard Branson (tentative)

Video Monitors
With Reminders

at All Entrances

And

Other Public Areas

Screensavers Mimic

Facility Wide

Reminders

Newsletters

Cyber Security Newsletter
Tips and Information to Protect
Your Patients, Workplace and Yourself
From the Office of David W. Loewy, PhD
Information Security Officer SUNY Downstate Medical Center

From SUNY Downstate's Chief Information Security Officer

Sent Campus Wide to all email address' Monthly to discuss issues that have immediate impact on individuals, both in-house and personal Issues.

This month the topic was IRS Scams. Next month will introduce a new android virus.

Other Awareness Activities

- Brownbag presentations

- Helpdesk support

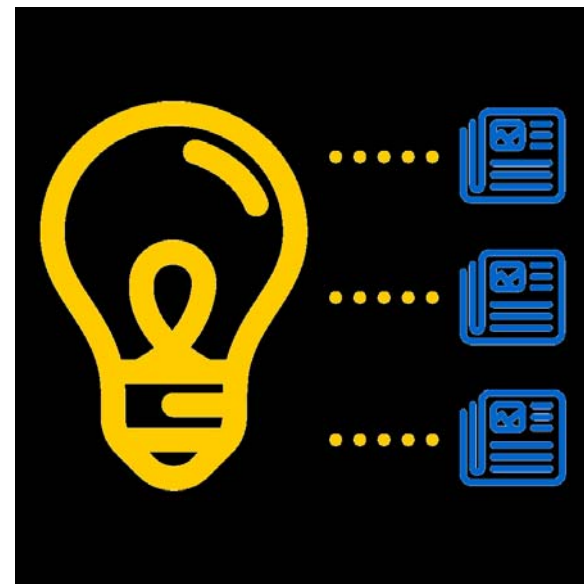- Institution wide email notifications

National, SUNY Statewide & Downstate Statistics

In Conclusion

As the use case for email communication matures, the practice of protecting email has been lacking.

Organizations need to take another look at their perceived protections, and perhaps view their approach differently.

David W. Loewy, PhD Chief Information Security Officer