The Brave New World of Cyber Breaches and Cyber Litigation

Jeff Bullwinkel, Associate General Counsel, Microsoft Europe
Susan Fahringer, Partner, Perkins Coie
Lorena Marciano, Director - EMEAR Data Protection and Privacy Officer, Cisco
Senior representative, GCHQ, National Cyber Security Centre

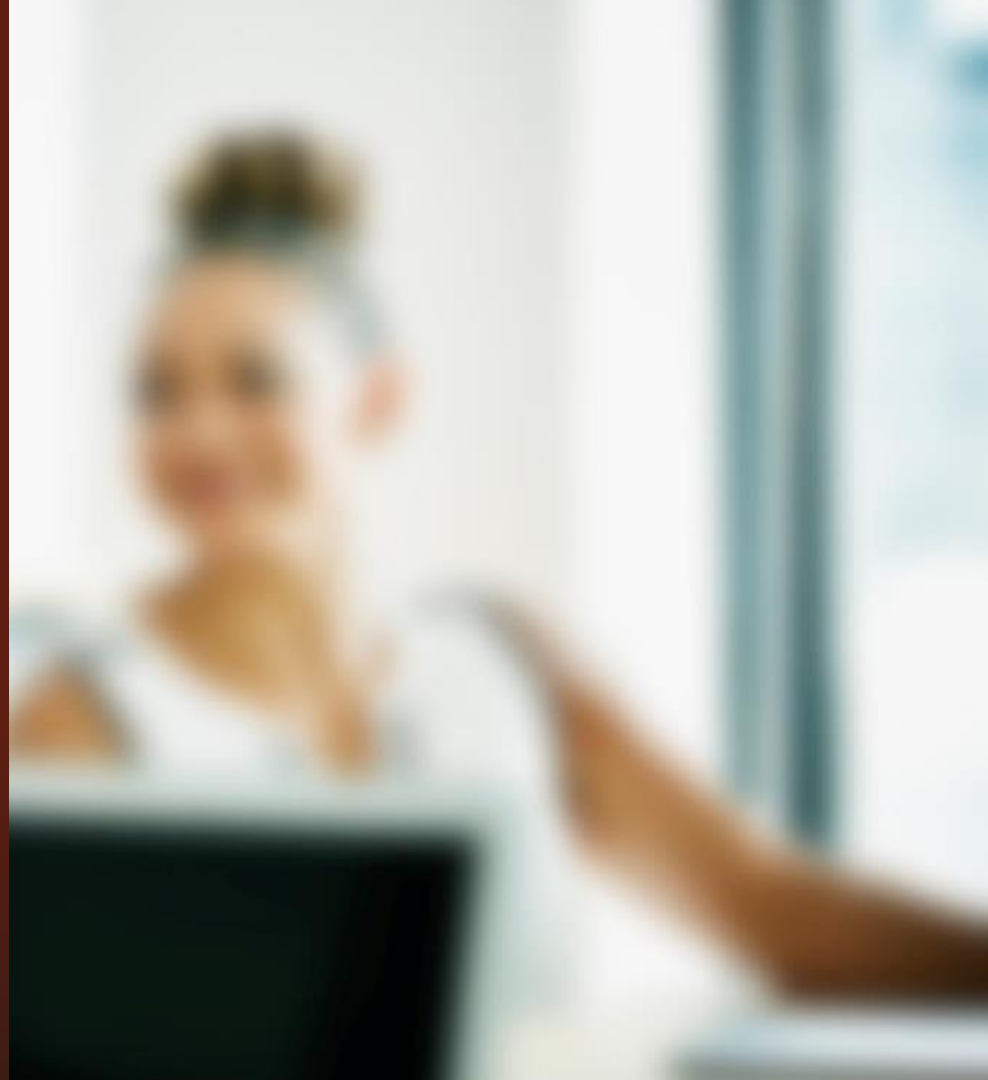
Agenda

1. The Scope, Breadth, and Nature of Cyberattacks Today
2. Public and Private Responses to these Attacks
3. The Legal and Litigation Landscape
4. Where to Go From Here

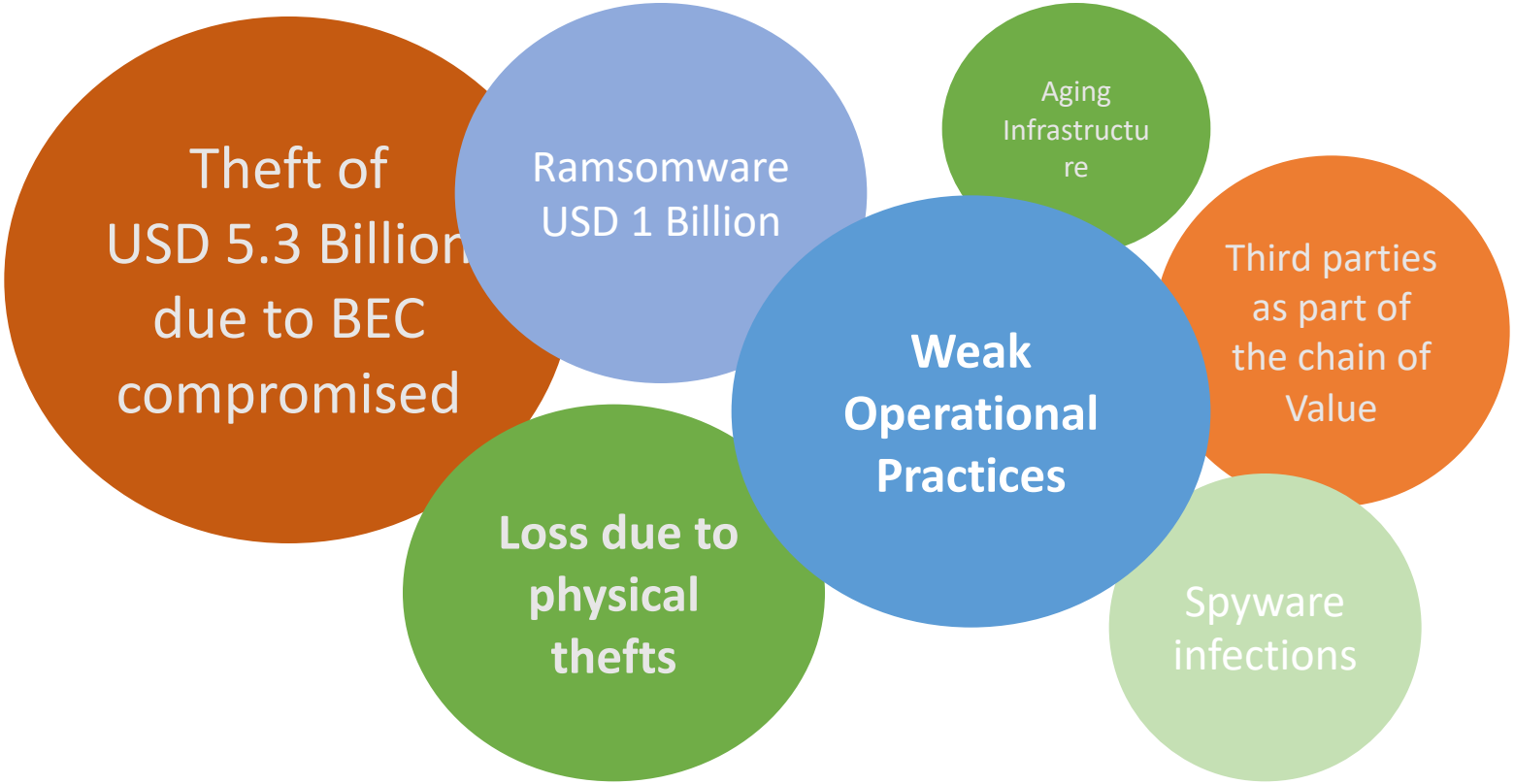
The digital world

Cybercrime

threatens it



Threats to Data



Cybersecurity

In the News, In the Boardroom

Increasing Level of Sophistication

Hacking as a hobby

Hacking for financial gain

Nation-state attacks

SOCIAL ENGINEERING

Cyber Weapons: The New Arms Race

The Pentagon's been hacked. The IMF has been hacked. Sony, Citigroup, Google—all victims of debilitating online attacks. It's war out there, and a scary new cyber-weapons industry is exploding to arm the combatants

by **Michael Riley** and **Ashlee Vance**
July 21, 2011 3:53 PM PDT
From **BloombergBusinessweek** | Subscribe | Reprints

In the early morning hours of May 24, an armed burglar wearing a ski mask broke into the offices of Nicira Networks, a Silicon Valley startup housed in one of the countless nondescript buildings along Highway 101. He walked past desks littered with laptops and headed straight toward the cubicle of one of the company's top engineers. The assailant appeared to know exactly what he wanted, which was a bulky computer that stored Nicira's source code. He grabbed the one machine and fled. The whole operation lasted five minutes, according to video captured on an employee's webcam. Palo Alto Police Sergeant Dave Flohr describes the burglary as a run-of-the-mill Silicon Valley computer grab. "There are lots of knuckleheads out there that take what they can and

An era of
invisible weapons

The New York Times

EUROPE

Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool

By NICOLE PERLROTH and DAVID E. SANGER MAY 12, 2017

SAN FRANCISCO — Hackers exploiting malicious software stolen from the National Security Agency executed damaging cyberattacks on Friday that hit dozens of countries worldwide, forcing Britain's public health system to send patients away, freezing computers at Russia's Interior Ministry and wreaking havoc on tens of thousands of computers elsewhere.

The attacks amounted to an audacious global blackmail attempt spread by the internet and underscored the vulnerabilities of the digital age.

Transmitted via email, the malicious software locked British hospitals out of their computer systems and demanded ransom before users could be let back in — with a threat that data would be destroyed if the demands were not met.

By late Friday the attacks had spread to more than 74 countries, according

Ambulance staff at a National Health Service hospital in London on Friday. Several hospitals across Britain were hit by a large-scale cyberattack, causing failures to computer systems. Andy Rain/European Pressphoto Agency

The New York Times

U.S.

In Computer Attacks, Clues Point to Frequent Culprit: North Korea

点击查看本文中文版

By NICOLE PERLROTH and DAVID E. SANGER MAY 15, 2017

SAN FRANCISCO — Intelligence officials and private security experts say that new digital clues point to North Korean-linked hackers as likely suspects in the sweeping ransomware attacks that have crippled computer systems around the world.

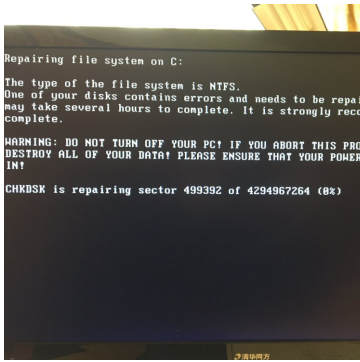
The indicators are far from conclusive, the researchers warned, and it could be weeks, if not months, before investigators are confident enough in their findings to officially point the finger at Pyongyang's increasingly bold corps of digital hackers. The attackers based their weapon on vulnerabilities that were stolen from the National Security Agency and published last month.

Adm. Michael S. Rogers, director of the National Security Agency, during a Senate Intelligence Committee hearing last week. Al Drago/The New York Times

More than
200,000 computers
in 150 countries





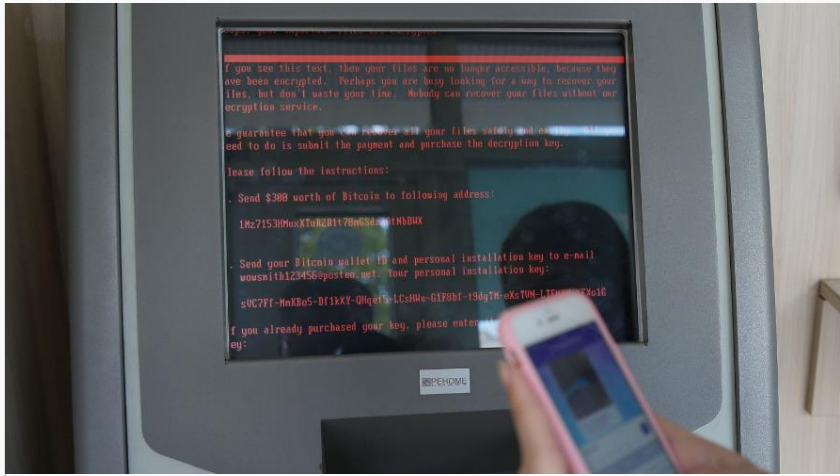


WANNACRY SOME MORE

The cyber attack that knocked out Ukraine this morning is now going global

By Max de Haldevang & Keith Collins | June 27, 2017

The ransomware that took out critical services in Ukraine this morning has now spread to computers worldwide with the help of leaked hacking tools allegedly developed by the US National Security Agency (NSA). The strain of ransomware being used in the attack is known as Petya, though some are calling it NotPetya due to disagreements over its core code. Petya/NotPetya has now hit Russia, Denmark, France, the United Kingdom, and the United States. Infected computers have their files locked, and the hackers demand users pay $300 in bitcoin to get them



Normally you ask ATMs for money. In cyber-attacked Ukraine, ATMs ask you. (Reuters/Valentyn Ogirenko)

Interfering with
political processes

euobserver

Microsoft warns EU on election hack threat

Europe Daily Bulletin No. 12198 — Agence Europe — 21 February 2019

> CONTENTS > PUBLICATION IN FULL > BY ARTICLE — 34 / 41

NEWS BRIEFS / JUSTICE

Microsoft warns against cyber attacks in the run-up to the European elections

The New York Times

Russian Hackers Targeted European Research Groups, Microsoft Says

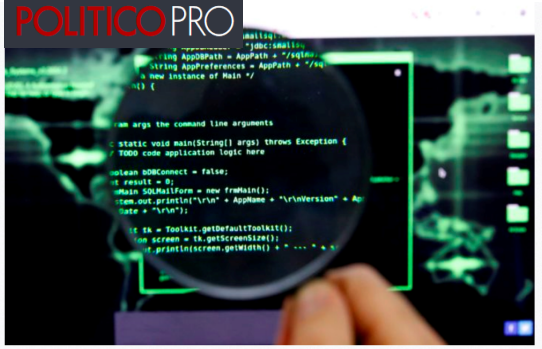
Handelsblatt

Mehrere Deutsche Institute von Hackerangriffen betroffen

Die Hackerangriffe sollen Microsoft zufolge zwischen September und Dezember 2018 erfolgt sein. Zugeordnet werden sie der Gruppe „Strontium“.

20.02.2019 - 14:53 Uhr • Kommentieren • Jetzt teilen

POLITICO PRO



Microsoft linked the hacking group Fancy Bear to the attacks | Jack Guez/AFP via Getty Images

Russian hackers attacked European think tanks, Microsoft says

The company is confident many of the attacks came from a group it calls ‘Strontium,’ better known as Fancy Bear.

By **LAURENS CERULUS** | 2/20/19, 5:00 AM CET | Updated 2/20/19, 5:06 PM CET

THE WALL STREET JOURNAL.

Europe Edition | March 24, 2019 | Print Edition | Video

Home World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate WSJ. Magazine

NEWSPLUS

Microsoft Says Russian Hackers Targeted European Non-[illegible]

By Donato Paolo Mancini

Feb. 20, 2019 3:51 a.m. ET | WSJ Pro

sky news

Microsoft spots Russian hacking campaign ahead of EU elections

According to Microsoft, the campaign is using the same tools which were used in an attempt to influence the US election in 2016.

Les Echos.fr

Cyberattaques : mise en garde de Microsoft avant les élections européennes

LUCAS MEDIAVILLA | Le 20/02 à 17:01 | Mis à jour à 17:16

pravda.ru

Microsoft сообщил об атаках хакеров на "институты Европы" и предложил новый сервис

Cyberspace is the new battlefield

THE VERGE

TECH \ CYBERSECURITY

UK hospitals hit with massive ransomware attack

Sixteen hospitals shut down as a result of the attack

by Russell Brandom | @russellbrandom | May 12, 2017, 11:36am EDT

A massive ransomware attack has shut down work at 16 hospitals across the United Kingdom. According to *The Guardian*, the attack began at roughly 12:30PM local time, freezing systems and encrypting files. When employees tried to access the computers, they were presented with a demand for $300 in bitcoin, a classic ransomware tactic.

The result has been a wave of canceled appointments and general disarray, as many hospitals are left unable to access basic medical records. At least one hospital has canceled all non-urgent operations as a result.

According to a statement from the National Health Service, the culprit is a ransomware strain known as Wanna Decryptor (also known as WannaCry). While operations at the hospitals have been severely impacted, there is no indication that patient data has been

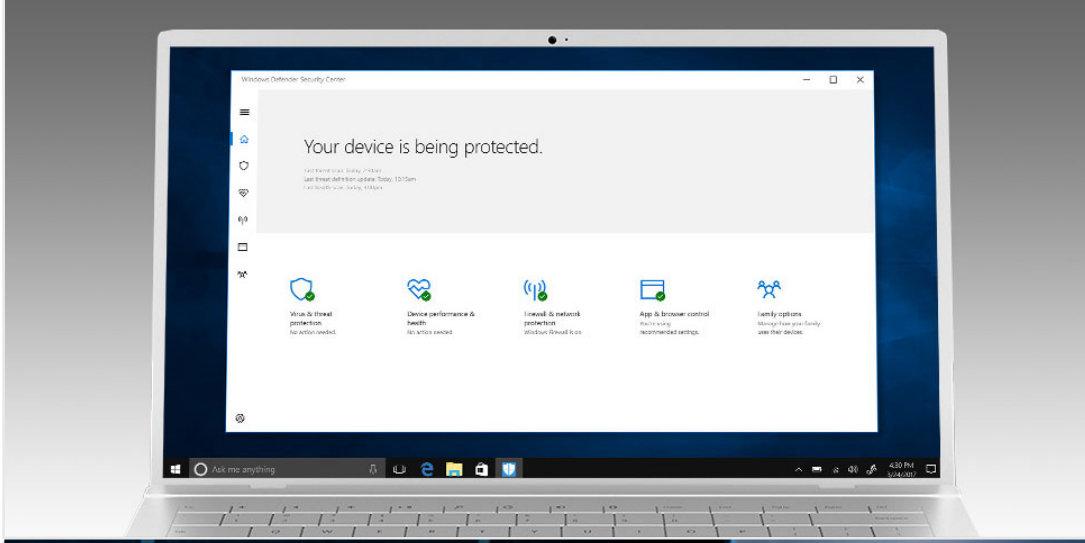
Peter O'Conner / Flickr

Attacking civilians
in times of peace

Video - Not-Petya Cyber-Attack & Wannacry
https://www.youtube.com/watch?v=1hIlTFG-RsU

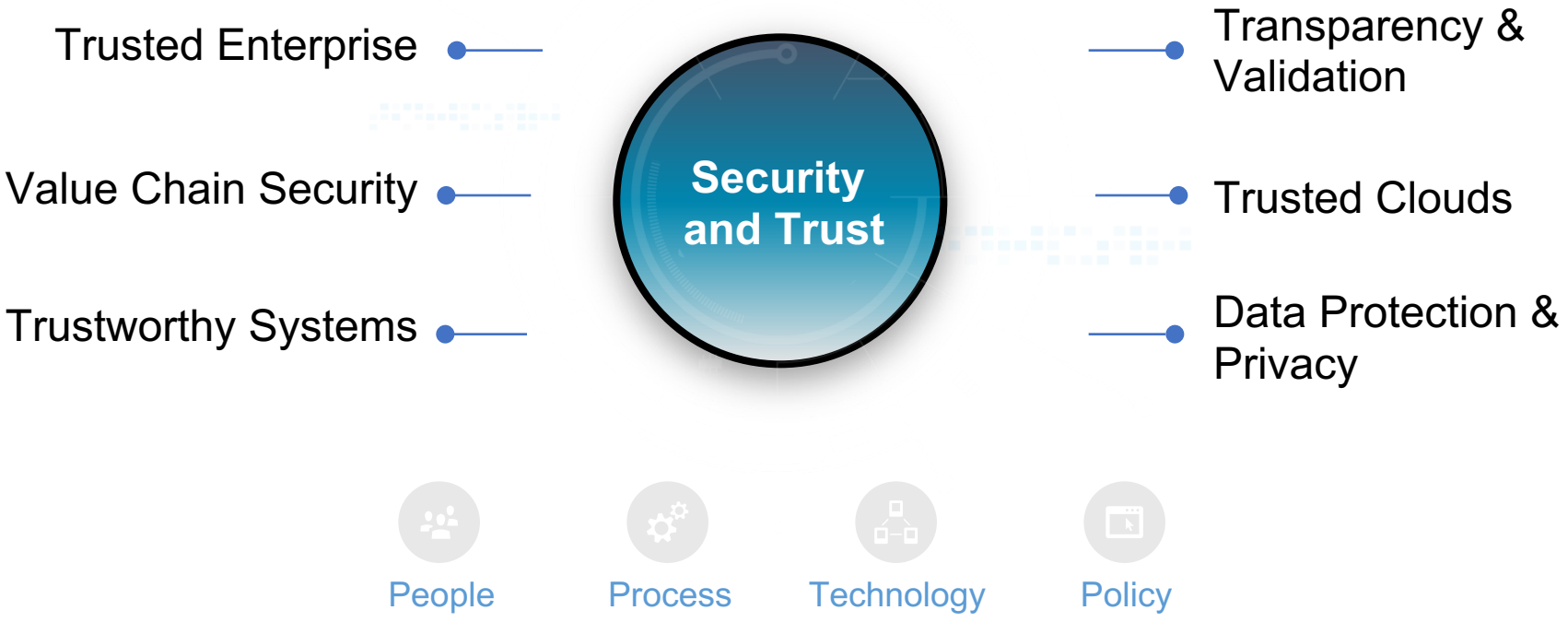
II. Public & Private Responses to these Attacks

The tech sector has the first responsibility

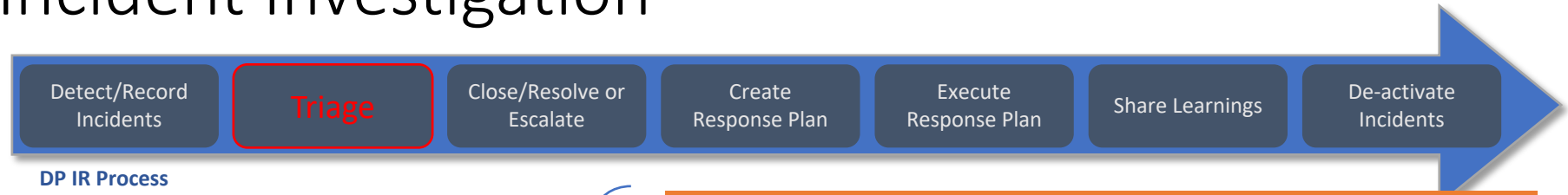


Our Comprehensive Approach

Creating a Trusted Digital Enterprise



Incident Investigation



DP IR Process

Triage Research:

What data was exposed?

When was it exposed?

How was it exposed?

How was it accessed?

Who viewed the data?

Finance/Capital Data:

- Financial Records, Bank Statements, Investor documents, Guarantees, Lease Agreements, Distributor/Partner Agreements…

Customer Data:

- Contracts, Device Configurations, Support, Installed Inventory

Personal data:

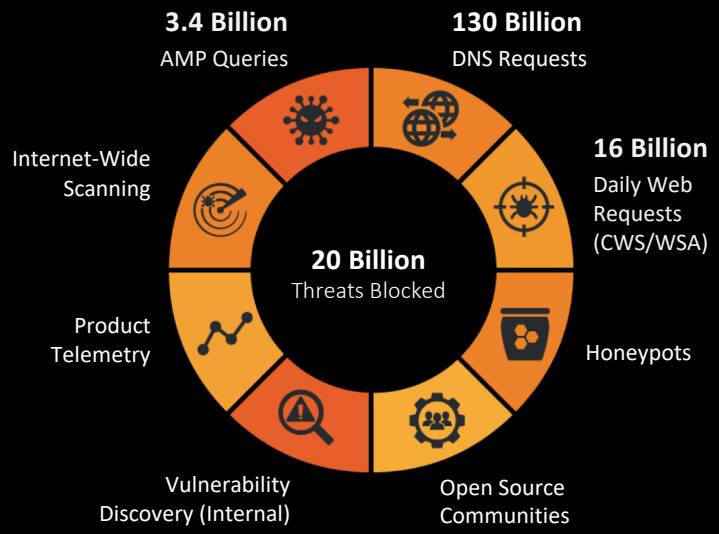
- PII: Name, Email, Address, Phone
- Sensitive PII: SSN, Drivers License, Passport, Visa, Bank Account
- Cisco: ID, Job Details, Job Location, Compensation, Diversity, Family

Intellectual Property:

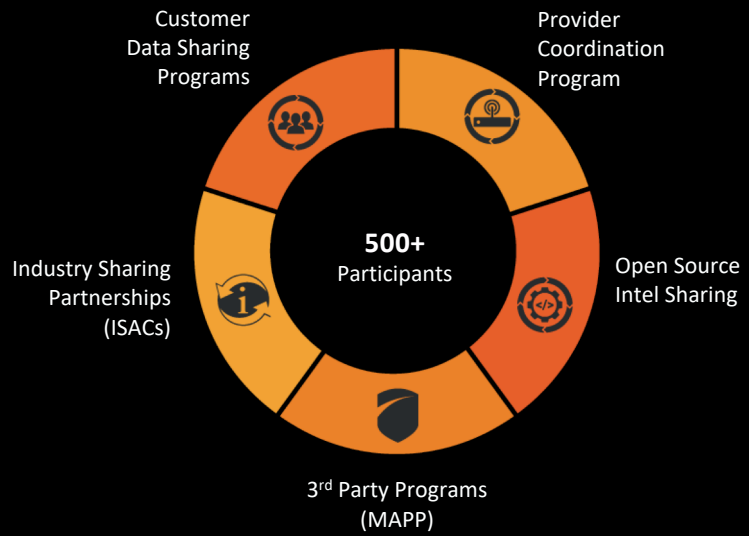
- Engineering Data, Source Code, Test Results, Org., Feature Roadmap, Manufacturing, Finance, Legal

Talos: Cisco security research

Threat Intel



Intel Sharing



300+
Full Time Threat Intel Researchers

Millions
Of Telemetry Agents

4
Global Data Centers

100+
Threat Intelligence Partners

1100+
Threat Traps

Security engineered-in and fully integrated

Identity & Access Management

Ensure only the right people have access to your organizational systems

Information Protection

Ensure documents and emails are viewed only by the intended recipients

Threat Protection

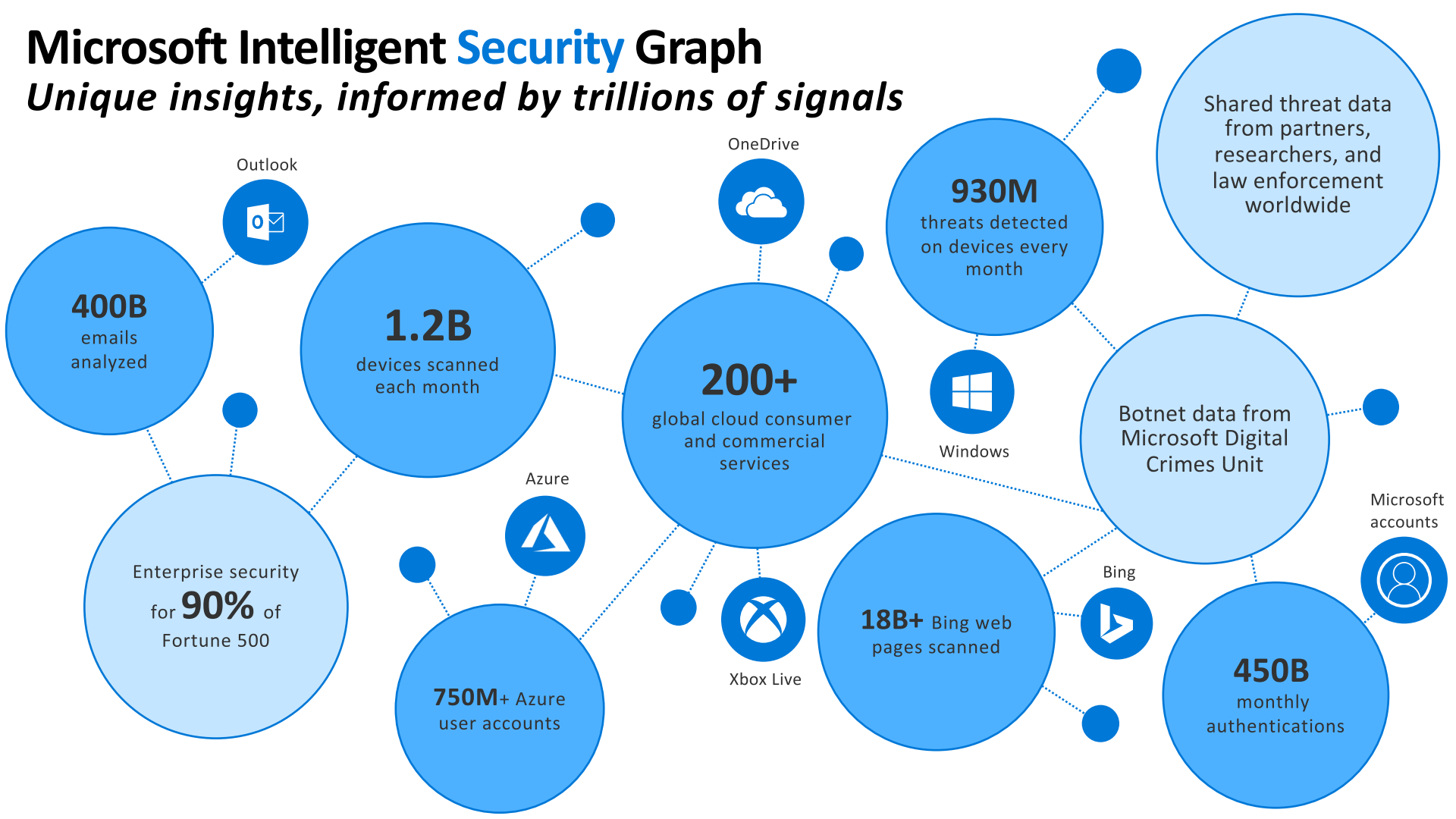
Thwart hackers and recover quickly if attacked

Security Management

Gain end-to-end visibility into your orgs security and manage security policy centrally

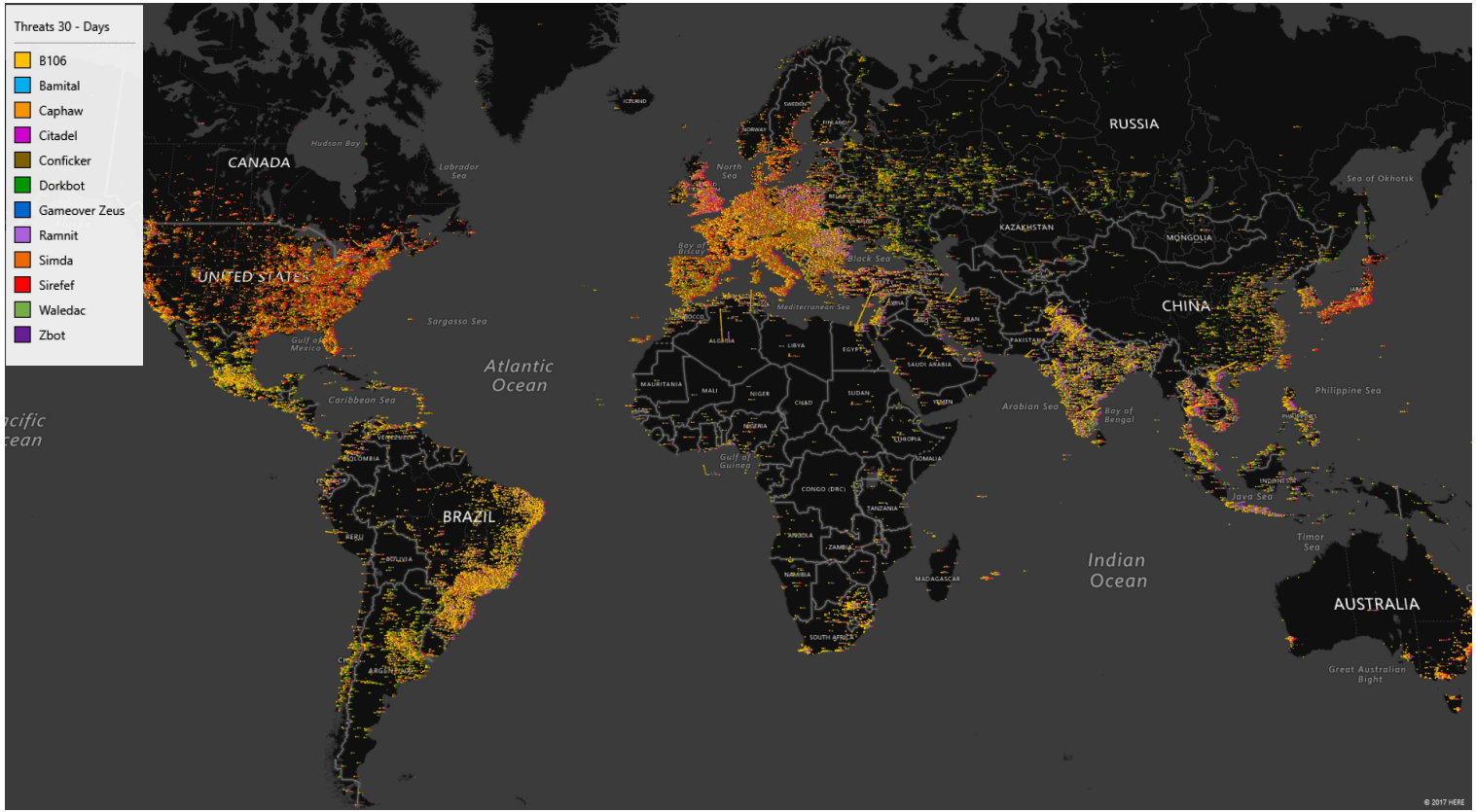
Microsoft Intelligent Security Graph

Unique insights, informed by trillions of signals



Combining technology and the rule of law

The Militarization of cyberspace



ZDNet

Iranian hackers suspected in worldwide DNS hijacking campaign

Mysterious group hijacks DNS records to reshape and hijack a company's internal traffic to steal login credentials.

By Catalin Cimpanu for Zero Day | January 10, 2019 -- 11:46 GMT (11:46 GMT) | Topic: Security

TC

Microsoft sues to take control of domains involved in Iran hacking campaign

Zack Whittaker @zackwhittaker / 2 days ago

The New York Times

Microsoft Seizes Websites It Traces to Iranian Hackers

Bloomberg

Cybersecurity

Microsoft Takes on Another Hacking Group, This One With Links to Iran

Company says court order has given it control of 99 web sites linked to group it calls Phosphorus

By Dina Bass
March 27, 2019, 12:11 PM EDT

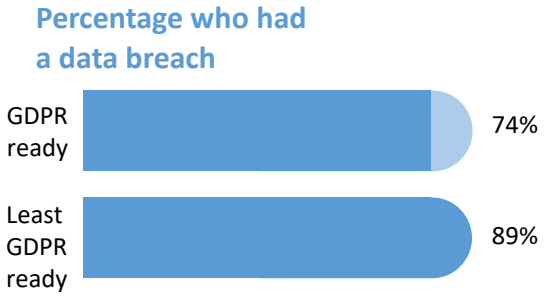
Microsoft Corp. said that it has taken control of 99 web sites used by a malicious group connected to Iranian hackers who attacked targets including g businesses in order to steal confidential information.

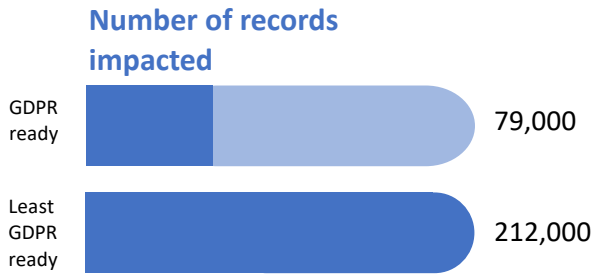
III. The Legal and Litigation Landscape

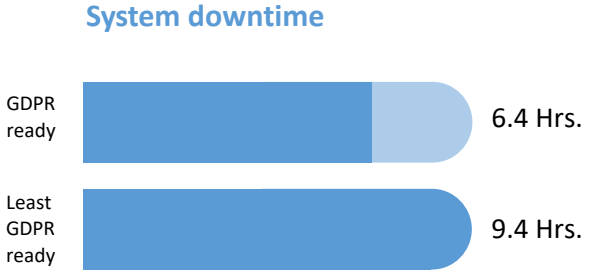
Cyber Legal Landscape

- GDPR
- NIS Directive
- Cyber Act
- E-Evidence/ CLOUD Act

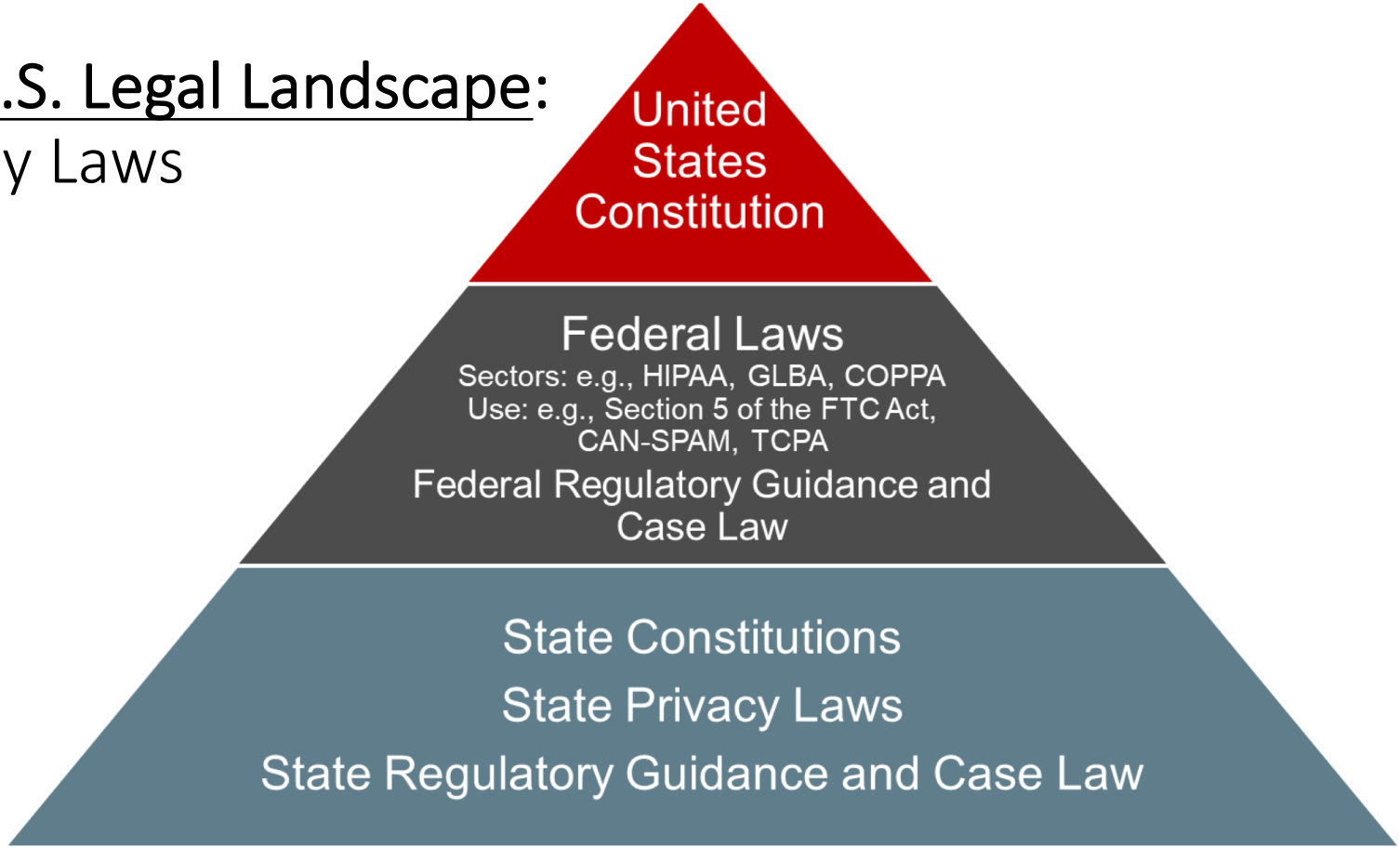
GDPR-ready companies have fewer and less costly breaches



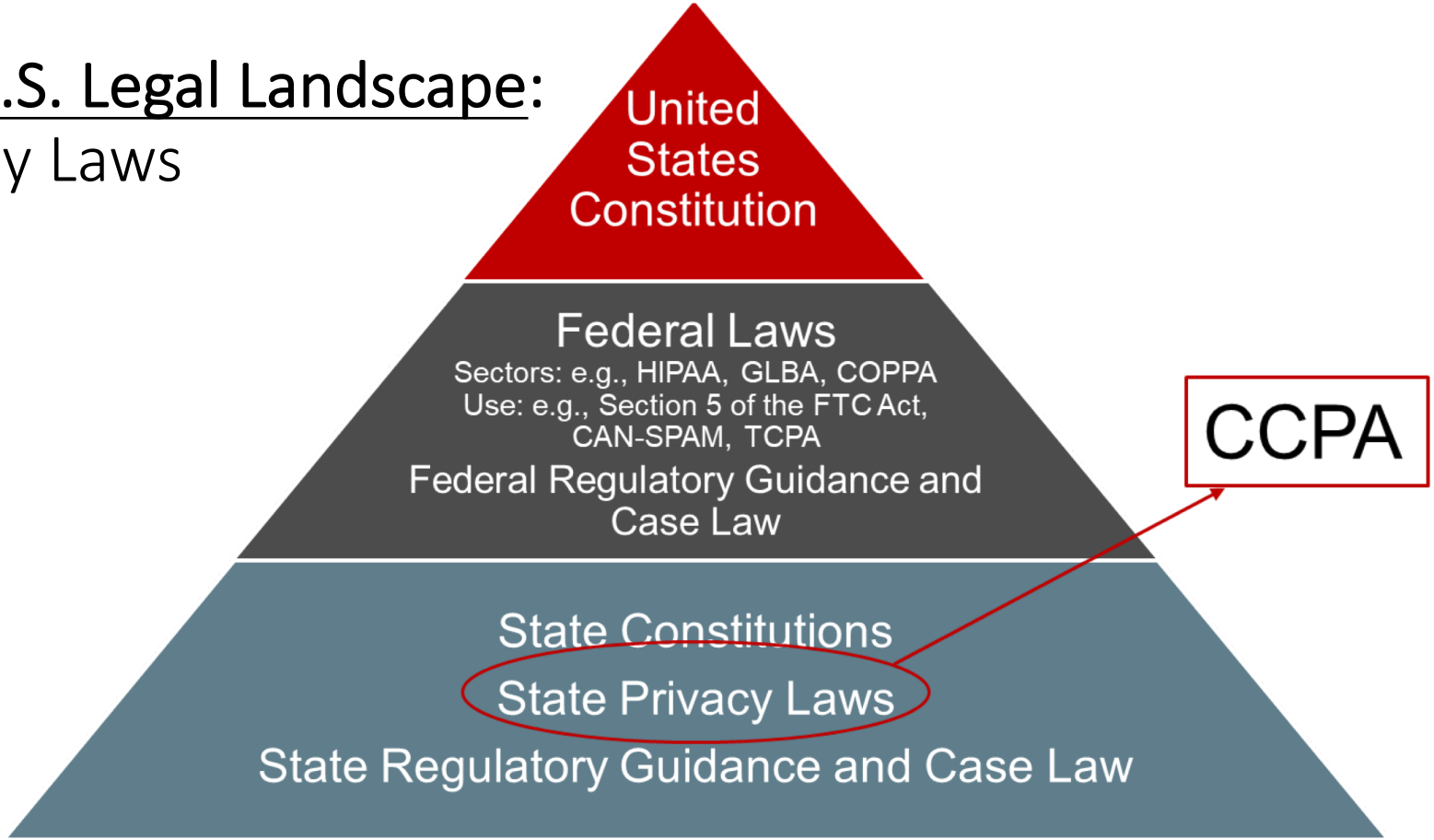




The U.S. Legal Landscape: Privacy Laws



The U.S. Legal Landscape:
Privacy Laws



Data Breach Litigation

- Regulatory Enforcement –
  Penalties, fines, litigation
- Private litigation –
  - Consumer vs. company
  - Card issuer/banks vs. company
  - Vendors vs. company
  - Shareholder derivative suits . . .

Best Practices

Be Prepared –

- Cyber insurance & risk allocation
- Internal Procedures
  - ✓ Data & Security Policies, Procedures & Standards
  - ✓ Risk Assessment
  - ✓ Incident Response Plan
  - ✓ Tabletop Exercise
- Pre-litigation Preparation

Best Practices

If litigation is filed:

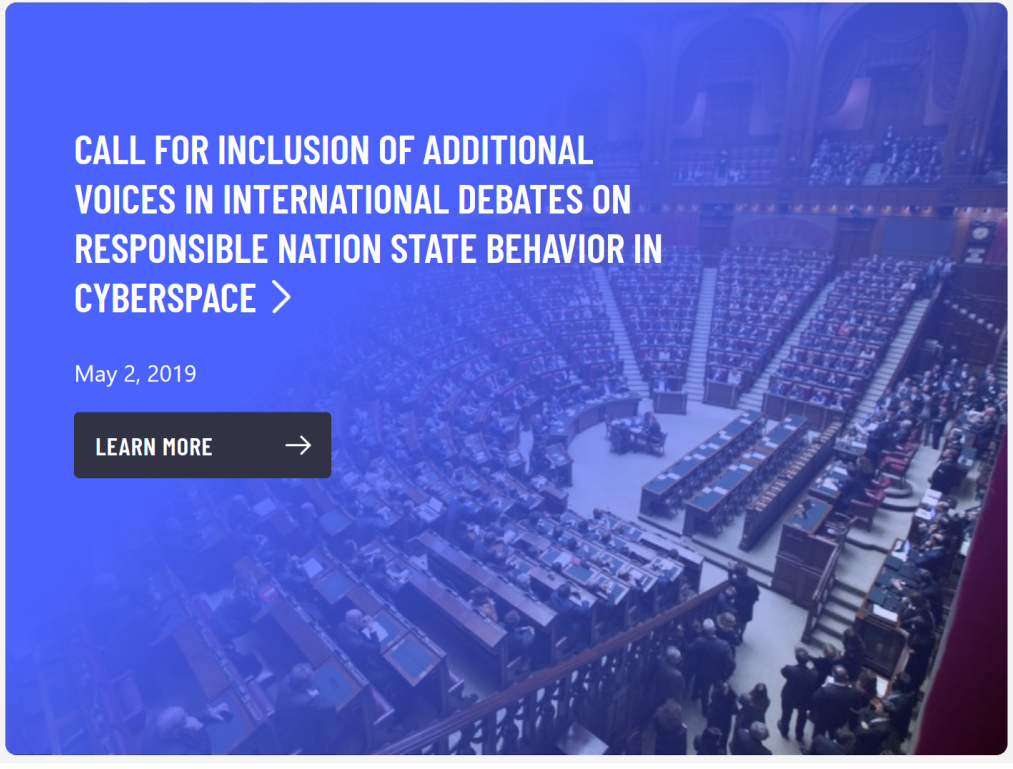
- Communications Plan
- Notices
- Evidence Preservation
- Privilege
- Managing multiple litigations

IV. Where To Go From Here

TECH ACCORD

About | Our Commitment | Policies & RFIs | Webinars | Events | Contact

WATCH VIDEO OVERVIEW



CALL FOR INCLUSION OF ADDITIONAL VOICES IN INTERNATIONAL DEBATES ON RESPONSIBLE NATION STATE BEHAVIOR IN CYBERSPACE >

May 2, 2019

LEARN MORE →

PROTECTING OUR ONLINE ENVIRONMENT IS IN EVERYONE'S INTEREST

We — as enterprises that create and operate online technologies — promise to defend and advanced its benefits for society.

LEARN MORE →

A global tech sector accord

Not help governments attack customers anywhere

Issue patches & protect customers everywhere

Partner to strengthen response to cyberattacks

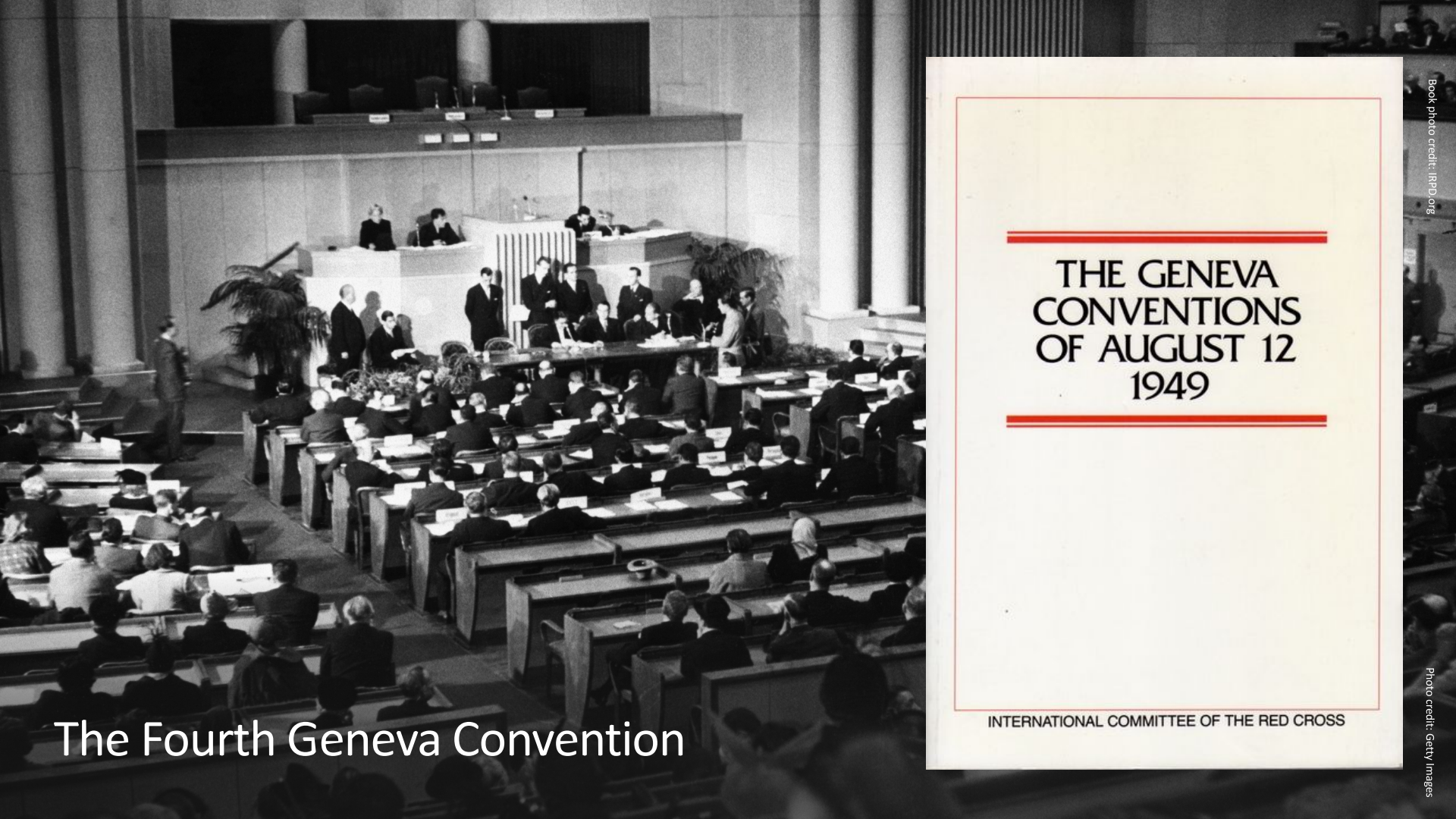
SIGNATORIES

ABB • ALITER • ANCHORFREE • ANOMALI • ARM • ATLASSIAN • AVAST • BALASYS • BILLENNIUM • BINARY HOUSE • BITDEFENDER • BT • CAPGEMINI • CARBON BLACK • CISCO • CLOUDFLARE • COGNIZANT • CONTRAST SECURITY • CYBER SERVICES • DATASTAX • DELL • DOCUSIGN • DOMAIN TOOLS • EBRC • ENTEL • ESET • EYEO • FACEBOOK • FASTLY • FIREEYE • FLOWMON NETWORKS • FRACTAL INDUSTRIES • F-SECURE • G DATA • GIGAMON • GITHUB • GITLAB • GLOBANT • GREYCORTEX • GUARDTIME • HITACHI • HP INC • HPE • IMPERVA • INTEGRITY PARTNERS • INTUIT • JUNIPER NETWORKS • KOOLSPAN • KPN • LINKEDIN • LIREX • MARK MONITOR • MEDIAPRO • MERCADO LIBRE • MICROSOFT • NIELSEN • NOKIA • NORTHWAVE • NTT • ORACLE • ORANGE • PALADION • PANASONIC • PANDA • PERCIPIENT.AI • PREDICA • ROCKWELL AUTOMATION • RSA • SAFETICA • SALESFORCE • SAP • SECUCLOUD • SILENT BREACH • SONDA • STACKPATH • STRIPE • STRONG CONNEXIONS • SWISSCOM • TAD GROUP • TANIUM • TELECOM ITALIA • TELEFONICA • TELELINK • TENABLE • THREATMODELER SOFTWARE INC • TREND MICRO • UNISYS • VMWARE • VU SECURITY • WISEKEY

We also need governments to act

Every government,
regardless of its policies or politics,
needs a national and global IT
infrastructure that it can trust.

Building on existing international law



The Fourth Geneva Convention

Book photo credit: IRPD.org

Photo credit: Getty Images

We need a
Digital Geneva
Convention

A Digital Geneva Convention

1.

No targeting of tech companies, private sector, or critical infrastructure

2.

Assist private sector efforts to detect, contain, respond to, and recover from events

3.

Report vulnerabilities to vendors rather than to stockpile, sell or exploit them

4.

Exercise restraint in developing cyber weapons and ensure that any developed are limited, precise, and not reusable

5.

Commit to nonproliferation activities to cyberweapons

6.

Limit offensive operation to avoid a mass event

Cyberspace now plays a crucial role in every aspect of our lives and it is the shared responsibility of a wide variety of actors, in their respective roles, to improve trust, security and stability in cyberspace.

We reaffirm our support to an open, secure, stable, accessible and peaceful cyberspace, which has become an integral component of life in all its social, economic, cultural and political aspects.

We also reaffirm that international law, including the United Nations Charter in its entirety, international humanitarian law and customary international law is applicable to the use of information and communication technologies (ICT) by States.

We reaffirm that the same rights that people have offline must also be protected online, and also reaffirm the applicability of international human rights law in cyberspace.

We reaffirm that international law, together with the voluntary norms of responsible State behavior during peacetime and associated confidence and capacity-building measures developed within the United Nations, is the foundation for international peace and security in cyberspace.

We condemn malicious cyber activities in peacetime, notably the ones threatening or resulting in significant, indiscriminate or systemic harm to individuals and critical infrastructure and welcome calls for their improved protection.

- Protecting the public core of the Internet
- Preventing proliferation of malicious ICT tools
- Promoting implementation of cyber norms and CBMs
- Preventing hack backs
- Protecting electoral processes
- Preventing cyberattacks on critical infrastructure
- Strengthening the security of products, processes and services
- Preventing ICT enabled theft of IP
- Advancing cyber hygiene

500+ endorsers of the Paris Call globally

Questions?