A VISUAL HISTORY OF CYBERSECURITY

1970

"Catch me if you can!"

2020

Future is looking Cloud-y
From the invention of ARPAnet in 1968, to the rise of personal computing in the 1980’s and telecommuting in the 21st century, this book examines the technological history that brought us here today. Cybercrime has evolved at a breakneck pace alongside the digital advancements of the past five decades, and cybersecurity and cyber professionals have been forced to adapt to a market of nonstop growth.

We hope this book provides a compelling visual snapshot of the history that led the cyber industry to where it is, along with our bold predictions for the future. To start, lets take a trip back to 1970...
1970
ARPANET, the precursor to the modern Internet, releases the Network Control Protocol (NCP) allowing computers at remote locations to transfer files between computers.

Published in 1970 and declassified in 1975, the 82-page Ware Report was authored by computer science legend Willis Ware and his team. The report outlined what were then largely theoretical weaknesses in networks. They’re now very real.

Shakey the robot, the first artificially intelligent mobile robot, is featured in National Geographic as an example of the future possibilities of computers. Receiving computer commands via radio link, Shakey used a TV camera, laser range finder and bump sensors to collect data.

The first computer virus is created by Bob Thomas as a non-malicious program that moves through computers displaying the message, "I am the Creeper, catch me if you can."

Funky Fact
The first four computer network nodes in ARPANET were all universities.

Don’t Fear the Reaper
Soon after the first virus, codenamed "Creeper," came the first anti-virus, appropriately named "Reaper."

"I was inducted into Carnegie Mellon University’s Robot Hall of Fame in 2004 alongside my robo-buds ASIMO and C-3PO."

Sources
1. www.ai.sri.com/shakey/; 2020
3. www.broadweb.ae/web/fascinating-evolution-cybersecurity/
5. A Visual History of Cybersecurity
6. 1970
7. 1980
8. 1990
9. 2000
10. 2010
11. 2020
12. PREDICTIONS
13. INSIGHTS
14. INTRODUCTION

ALSO 1970
Published in 1970 and declassified in 1975, the 82-page Ware Report was authored by computer science legend Willis Ware and his team. The report outlined what were then largely theoretical weaknesses in networks. They’re now very real.
1971

John Draper legendarily discovers a method to unlock free long distance calls using a 2600 hertz frequency tone produced by a toy whistle found in Cap’n Crunch cereal boxes. This “phreaker” subculture fostered influential digital visionaries like Jobs and Wozniak, who were once phone phreakers themselves.³

1975

Paul Allen and Bill Gates, two friends, form their own software company, Microsoft.¹

1971

The “floppy disk” is invented by Alan Shugart and a team of IBM engineers, allowing data to be shared among computers.²

Sources
2 www.livescience.com/20718-computer-history.html ; 2017
3 www.worldsciencefestival.com/infographics/a_history_of_computer_science/
**1976**

**INSIDER ATTACK**

Greg Chung of Boeing commits one of the worst cybersecurity breaches in history, sending $2 billion **worth of stolen documents** to China.

The binders contained thousands of documents, including many design manuals related to U.S. military aircraft—the B-1 bomber, the C-17 military cargo plane, the F-15 fighter jet, and the Chinook 47 and 48 helicopters.¹

*It was like walking into King Solomon’s mine.*¹

---

**2006**

The FBI begins their investigation into Chung’s possible espionage involvement.

---

**2010**

Chung is sentenced to 15 years for hoarding and sharing sensitive information.

---

**1979**

**XEROX PALO ALTO RESEARCH CENTER**

At the Xerox Palo Alto Research Center, John Shoch and Jon Hupp create a small program that searches a network for computers with idle processor time, the first **worm**.

Ironically, the first worms were intended to provide more efficient use of computers.

Worms demonstrated a capacity for invading any computer on a network, creating the **security threat that continues with viruses today.**²

Sources:

1. www.newyorker.com/magazine/2014/05/05/a-new-kind-of-spy

2. www.technovelgy.com/ct/content.asp?Bnum=190

---


PERSON OF THE YEAR

THE COMPUTER MOVES IN

1980
There she blows

1980
IBM ignites the personal computer market and revolutionizes business computing with widespread industry adoption. Formerly known as the IBM Model 5150, their first PC used Microsoft’s MS-DOS operating system and a 4.77 MHz Intel 8088 microprocessor.

FUN FACT
The popular video arcade game “Pac-Man” is released in 1980. The original Japanese title of Puck Man was changed to Pac-Man for international releases as a preventative measure against defacement of the arcade machines by changing the P to an F.

1981
The first video game magazine in the U.S. is founded and called Electronic Games. After rapid success during its first two years, it faltered during the 1983 Video Game Crash and ceased publication in 1985.

1982
Commodore’s VIC-20 home computer becomes a less expensive alternative to their initial PET PC and is the first PC to sell more than one million units. Star Trek star William Shatner appeared in their advertisements.

The U.S. reprograms computer equipment that was being purchased through a front company for a Soviet gas pipeline. This proto-cyberattack causes the pipeline to explode.

Sources
1 www.computerhistory.org/timeline/1980/ ; 2020
2 www.gcn.com/Articles/2013/05/30/GCN30-Timeline-Cybersecurity.aspx?Page=1 ; 2013
1984
Apple’s iconic “1984” commercial airs on January 22, 1984 during Super Bowl XVIII. Apple introduces the Macintosh.¹

1985
Microsoft releases Windows-1.²

1986
Markus Hess and his accomplices are arrested in West Germany for hacking into the Lawrence Berkeley National Laboratory and selling stolen information to the KGB, but only receive suspended sentences.³

1987
President Reagan signs the Computer Security Act of 1987 to protect the computer data of federal agencies.³

Sources
1. www.computerhistory.org/timeline/1984/ ; 2020
2. www.worldsciencefestival.com/infographics/a_history_of_computer_science/

DOUBLE DISASTER
The Chernobyl nuclear reactor explodes in the USSR. The Space Shuttle Challenger disaster takes place when the space shuttle disintegrates after being launched, killing all on board.
Viruses became more problematic and widespread following the Morris worm. The first dedicated antivirus company is also founded this year.

1988

Robert Morris' self-propagating computer worm succeeded in closing down much of the internet and led to a felony conviction. He received a sentence of three years of probation, 400 hours of community service and a $10,050 fine.

HI! MY NAME IS ROBERT MORRIS

“The Morris Worm] woke the public up to the need for cybersecurity. Prior to the invasion of the worm, no attack had affected so many private users and companies at once.

Although the inflicted damage was an accident, Morris was the first person to ever be convicted under the 1986 Computer Fraud and Abuse Act.”

Sources:

Image: www.flickr.com/photos/intelfreepress/1047720993/; 2013
1 www.sentinelone.com/blog/history-of-cyber-security/
2 www.captechu.edu/blog/cyber-security-impact-30th-anniversary-of-morris-worm
THE MORRIS WORM CLOSED DOWN MOST OF THE INTERNET WHILE IT WAS ACTIVE...

SORRY, INTERNET IS CLOSED
A U.S. Air Force research facility discovers a password "sniffer" was installed onto their network, compromising over 100 user accounts. The two hackers responsible were identified as Cowboy and Kuji, working together under the name Datastream.  

Netscape develops Secure Sockets Layer encryption to ensure safer online transactions in response to internet security concerns.

Marc Andresson creates the first user-friendly web browser under the name Mosaic (later known as Netscape.)

Arpanet starts the operational network known as the Internet, connecting approximately 2.6 million people worldwide.

HTTPS://

Sources:
1. www.gcn.com/Articles/2013/05/30/GCN30-Timeline-Cybersecurity.aspx?Page=1; 2013
2. www.cybersecurityventures.com/cybersecurity-ceo-the-history-of-cybercrime-from-1834-to-present/; 2019
1995

The first Microsoft Word virus spreads worldwide via macro commands.

1996

President Clinton initiates the President's Commission on Critical Infrastructure Protection.

1996

Health Insurance Portability and Account Act (HIPAA), becomes law on August 21, 1996.

1996

Russian software engineer Vladimir Levin hacks Citibank’s New York IT system, illegally wiring an estimated $10 million to accounts worldwide from his apartment in Saint Petersburg.

FishNet Security is founded, one of two companies which later merge to form Optiv.

Sources
Image: Bob McNeely, The White House (Public Domain)

1 www.cybersecurityventures.com/cybersecurity-and-the-history-of-cybercrime-from-1834-to-present ; 2019
2 www.pbs.org/legendaryaccounts/facilities/stories/cyberone/flags.html ; 2003
Teenage hackers gain control of hundreds of computer systems used by the military, government and private sectors and steal a piece of NASA software in an incident known as the "Solar Sunrise." Systems are shut down for three weeks.¹

Max Butler is imprisoned for 18 months after hacking U.S. government websites in 1998.³

"He's so good, the FBI asks for his help. But life as a "white hat hacker" isn't exciting enough for Max Butler."²

Once released in 2003, he commits attacks, programs malware and steals credit information using the internet.³

In 2007 he is arrested again and pleads guilty to wire fraud, stealing millions of credit card numbers and executing nearly $86 million in fraudulent purchases.³
IT teams rushed applications onto the web during this time, prioritizing speed-to-deployment, scalability, availability and usability over security.

The Melissa Virus infects Microsoft Word documents and automatically disseminates itself as an attachment to the first 50 names in an infected computer’s Outlook email address list, $80 million in total damages.¹

Enterprise Security is born²
Earthworms can grow up to 9.8 feet (3 meters) in length.¹

The ILOVEYOU worm, a.k.a. love bug, infects government and private systems worldwide. In response, the U.S. pushes for the Council of Europe Cybercrime Treaty, to harmonize computer crime laws among nations.²

USB flash drives, also known as jump drives, memory sticks or thumb drives, enter the market. This new form of portable storage consists of flash memory paired with an integrated USB interface. They quickly replace CDs and floppy disks due to their smaller size, quicker read/write speeds, increased storage capacity and greater durability.⁴

A hacker attempts to extort $100 thousand from an internet music retailer after stealing customers’ credit card information. The retailer refuses to pay, prompting the hacker to post the customers’ credit card info.³

A 15-year-old Canadian high school student named Michael Calce, a.k.a. MafiaBoy, performs a distributed denial of service (DDoS) attack on several prominent websites, causing an estimated $1.2 billion in damages.¹

2000

A Visual History of Cybersecurity

Sources
2. www.gcn.com/Articles/2013/05/30/GCN30-Timeline-Cybersecurity.aspx? ; 2013
3. www.welcomewildlife.com/all-about-earthworms/#:~:text=Earthworms%20vary%20widely%20in%20size,feet%20(3%20m)%20long! ; 2020
5. www.pbs.org/wgbh/pages/frontline/shows/cyberwar/etc/faqs.html ; 2003
2001

Code Red worm is Unleashed

Carbonated Fact
Named code red because the discoverers were drinking Mountain Dew Code Red when they found the worm.1

July 13th, 2001
CODE-RED VERSION 1 RELEASED.1

August 9th, 2001
ITS ALL OVER.

July 19th, 2001
CODE-RED VERSION 2 RELEASED.1

359 THOUSAND
devices infected in just
15 HOURS.1

2001
Microsoft releases
Windows XP operating system.3

2001
Apple releases iTunes, a media player and library.2

2002
The thirteen Domain Name System (DNS) root servers are targeted by an hour-long DDoS attack, though most internet users are unaffected.4

2003
The Department of Homeland Security (DHS) begins operations and creates the National Cybersecurity Division.4

1 Million
of the 5.9 million
Microsoft IIS web servers were infected1

Estimated worldwide cost of Code Red
$2.6 Billion1

Sources
1 www.caida.org/research/security/code-red/#background
2 www.sans.org/reading-room/whitepapers/dlp/paper/874#:~:text=The%20Code%20Red%20worm%20cost,were%20infected%20by%20Code%20Red
3 www.computerhistory.org/timeline/2001/ ; 2020
4 www.cybersecurityventures.com/cybersecurity-ceo-the-history-of-cybercrime-from-1834-to-present/ ; 2019

2002
INTERNET ATTACK

2003
OPTIV HISTORY

2002: The other half of what later became Optiv, Accuvant, is founded.

2001
INTERNET ATTACK

A Visual History of Cybersecurity
FOR THOSE WHO WISH TO PLAY IN THE SHADOWS

2003

ALBERT GONZALES IS ARRESTED IN 2003 FOR HIS ROLE IN SHADOWCREW

ShadowCrew was a group which stole credit and debit card information and sold it online. Gonzales begins working with authorities in exchange for his freedom. From 2006 until his arrest in 2008, he takes part in another string of credit and debit card thefts targeting TJX, Heartland Payment Systems and a prominent bank, netting him millions of dollars.¹

2008

OPERATION CYBER SWEEP

The United States Justice Department announces Operation Cyber Sweep, which results in more than 70 indictments and 125 convictions or arrests for cyber crimes and fraud, including hacking, phishing and spam.¹

Sources:
¹ www.cybersecurityventures.com/cybersecurity-ceo/the-history-of-cybercrime-from-1834-to-present/; 2019
The hacker group "Anonymous" forms. It is a loose association of "hacktivists", activist hackers, who initially targeted websites in protest or as publicity stunts. Over time, they broadened their targets to include government agencies. Members of the group are referred to as "Anon" and often wear Guy Fawkes masks in public.\(^1\)

Brain Salcedo attempts to steal customer credit card information from a major home improvement retailer and is sentenced to 9 years.\(^2\)

O’Reilly Media launches the Web 2.0 Conference, popularizing the term "Web 2.0" in reference to a new type of website emphasizing user-generated content in a virtual community. Typical Web 2.0 sites include blogs, wikis, social media sites or image and video sharing sites.\(^3\)

A 41-year-old Nigerian citizen targets a consumer data broker and compromises data on 163 thousand customers. Initially only 35 thousand people were informed of the breach, but media pressure later revealed an additional 128 thousand people were affected.\(^4\)

Spirit Rover arrived on Mars in Jan 2004. NASA has since hacked it multiple times.\(^1\)

Sources
The so-called “data breach epidemic” begins. 157 data breaches are publicly reported this year, including the first leak of over 1 million credit card records. By 2017, that number increased tenfold to 1,579 data breaches.¹

Cybersecurity Ventures expects that businesses will fall victim to a ransomware attack every 11 seconds by 2021, up from every 14 seconds in 2019 and every 40 seconds in 2016.²

Damage related to global cybercrime is projected to hit $6 trillion annually by 2021.³ The complete FY2021 federal budget for the United States is $4.8 trillion.³ Of which $18.78 billion is reserved for all cybersecurity funding.⁴

Sources
1  www.securityboulevard.com/2018/03/the-data-breach-epidemic-no-info-is-safe/ ; 2018
2  www.cybersecurityventures.com/cybersecurity-market-report/ ; 2019
3  www.thebalance.com/u-s-federal-budget-breakdown-3305789 ; 2020
2005
The Canadian Anti-Fraud Centre reports over 11 thousand identity theft complaints with losses totalling $8.5 million.

2006
Hadoop 0.1.0 is released. Hadoop is a collection of open-source software utilities developed by the Apache Software Foundation which provide a framework for a cluster of computers to process big data efficiently. It can automatically handle hardware failures as it was built with the assumption that these are common occurrences. It quickly saw widespread adoption, with more than half of Fortune 50 companies using it by 2013.

2006
Cybercriminals steal the information of 4.5 million credit and debit cards from a large, Massachusetts-based retailer.

2006
A Veteran’s Affairs Department (VA) laptop containing records on 26.5 million active duty military and veterans is stolen during a burglary.

2006
Amazon releases Elastic Compute Cloud. This popularizes what becomes known as cloud computing, a service model where users have on-demand access to computing resources without the need to manage them.

Identity theft is the fastest growing form of consumer fraud in North America.

The site and its founder, Julian Assange, became world famous after the release of over 200 thousand United States diplomatic cables in 2010.

Sources:
2007

Arash Ferdowsi and Drew Houston founded Dropbox, a cloud storage service.1

Hitachi announces the first terabyte hard disk drive.1

2008

Anonymous targets the Church of Scientology’s website with 500 DDoS attacks in one week as part of an activist movement called “Project Chanology.”2

A United States Central Command employee inserts a flash drive into their laptop, accidentally releasing a worm into classified and unclassified systems. This breach, known as “Operation Buckshot Yankee” and delivered by a foreign intelligence agency, is the worst to date and prompts the Department of Defense to revamp their cyber defense strategy.3

2009

Satoshi Nakamoto, whose true identity remains unknown, releases the source code for Bitcoin. Bitcoin is a decentralized digital currency based on blockchain technology known as cryptocurrency.1

A series of cyber attacks, known as the Aurora attacks, target Google and 33 other companies in an attempt to steal intellectual property. The group, reportedly operating out of China, continues to target defense-related and other organizations.2

Mobile data speeds get a boost from the widespread adoption of 3G networks.3

Sources
1 www.computerhistory.org/timeline/ ; 2020
3 www.gcn.com/articles/2013/05/30/014205-Timeline-Cybersecurity.aspx?Page=1 ; 2013
A cybercrime ring steals $70 million from banks in the United States with the Zeus Trojan malware, diverting the money to Eastern Europe before being caught. 3

United States and Israeli intelligence services co-develop the Stuxnet worm, designed to sabotage Iran’s nuclear program. It is considered the first weaponized malware. 1

What is Trojan Malware?

Trojan Horse software, or a Trojan virus is a type of malware that is disguised as legitimate software. 4

Stuxnet didn’t work like other worms and viruses before it. Instead of only stealing information, the virus physically affected the computers it infected. 2

It works in two ways:

1. Spam Messages
2. Drive-By Downloads

Sources:
A group of five Eastern European hackers steal press releases from several newswire agencies before they can be announced.¹

Millions of email addresses are compromised in a cyberattack on Epsilon, which provides email and marketing services to their clients.²

A splinter group of the hacking collective Anonymous, known as Lulz Security or LulzSec, targets Fox.com and Sony’s Playstation Network (PSN) among 250 public and private organizations. Through these attacks, they gain access to the credit card information of over 100 million PSN users, costing Sony more than $170 million. They publicize these hacks through Twitter to shame owners for their insufficient security.²

Attackers with Chinese IP addresses expose the personal information of 35 million South Koreans by uploading malware to a server which updates ESTsoft’s ALZip compression software. The hackers gain access to names, birthdates, genders, telephone numbers, street and email addresses, user IDs and hashed passwords.²

Sources
² cybersecurityventures.com/cybersecurity-ceo-the-history-of-cyber-crime-from-1834-to-present/ ; 2019
The Internet of Things

2011

Nest Labs releases their Nest Learning Thermostat as part of the nascent Internet of Things. The Nest uses machine learning to adapt to a user's preferences and save energy when no one is home.¹

1 in 10

enterprises now use ten or more AI applications; chatbots, process optimization and fraud analysis lead a recent survey's top use cases.³

2011

Apple releases the iPhone 4S with a built-in, voice-activated personal assistant named Siri.²

By 2025—more than 75 billion IoT devices will be connected to the web.⁴

2011

The United States announces the National Strategy for Trusted Identities in Cyberspace, an initiative to foster trust between individuals and organizations on the internet.¹

2012

The Raspberry Pi is released by the foundation of the same name. This small computer is easy to use and simple to program, making it extremely popular among hobbyists and students.⁴

References:
¹ www.computerhistory.org/timeline/2011/ ; 2020
³ www.forbes.com/sites/louiscolumbus/2020/06/04/10-ways-enterprises-are-getting-results-from-ai-strategies/#606d8f386fdb ; 2020
⁴ www.opensource.com/resources/raspberry-pi
Yahoo suffers the largest data breach in history, affecting all three billion user accounts. The company failed to report the breach until 2016, leading to a $35 million dollar fine from the Securities and Exchange Commission (SEC).\(^1\)
Andrew Komarov, CIO of the cybersecurity firm InfoArmor, had been helping Yahoo! and law enforcement in response to the Peace data. In trying to track down the source of Peace’s data, he discovered evidence of this latest breach from a dark web seller offering a list of more than one billion Yahoo! accounts for about $300 thousand in August 2015.

The first data breach occurred on Yahoo! servers in August 2013; Yahoo! stated this was a separate breach from one which occurred in late 2014 and was conducted by an “unauthorized third party”. Yahoo! reported the breach on December 14, 2016, and forced all affected users to change passwords, and to reenter any unencrypted security questions and answers to make them encrypted in the future.

In February 2017, Yahoo! notified some users that data from the breach and forged cookies could have been used to access these accounts. This breach is now considered the largest known breach of its kind on the Internet.

In December 2016, it was learned that an even bigger breach took place in August 2013.

During the second half of 2016, Yahoo! reported two major data breaches perpetrated by hackers.

September 2016, the company said that at least 500 million of its accounts were hacked in 2014 by what it believed was a state-sponsored actor.

In December 2016, it was learned that an even bigger breach took place in August 2013.

In October 2017, Yahoo! updated its assessment of the hack, and stated that it believes all of its 3 billion accounts at the time of the August 2013 breach were affected.
2013

Former CIA employee and NSA contractor Edward Snowden leaks hundreds of thousands of documents from multiple confidential national security programs. Included was PRISM, a program where the NSA collected data with the assistance of Facebook, Google and Microsoft. These leaks divided the United States and caused many to lose trust in the government.

In the wake of the Snowden leaks, President Obama requests $769 million to improve the Department of Homeland Security’s information security.

A subject of controversy, Snowden has been variously called a hero, a whistleblower, a dissident, a patriot and a traitor.

Sources
1 www.varonis.com/blog/events-that-changed-cyber-security/ ; 2020
Sources

1. www.computerhistory.org/timeline ; 2020
2. www.cybersecurityventures.com/cybersecurity-ceo-the-history-of-cybercrime-from-1834-to-present/ ; 2019
A flaw in the OpenSSL cryptographic library known as the Heartbleed bug is discovered. Almost 20% of web servers worldwide were vulnerable to this bug, which allowed hackers to spy on communications and steal usernames, passwords, emails, instant messages and confidential files. The Fixed OpenSSL library largely reduced the effectiveness of this exploit.

Ironically, companies who were running a version of OpenSSL more than two years old in April 2014 were not affected by the Heartbleed bug.

Sources:
1. www.computerhistory.org/timeline/; 2020
Optiv was able to offer a comprehensive suite of end-to-end solutions across all phases of the cybersecurity lifecycle.
2015

A worldwide group of cybercriminals hacks a database of prepaid debit cards and uses the data to steal $45 million from ATMs around the world.

Sources:
1. www.cybersecurityventures.com/cybersecurity-ceo-the-history-of-cybercrime-from-1834-to-present/ ; 2019
2. www.varonis.com/blog/events-that-changed-cybersecurity/ ; 2020

2015

Hackers steal 4.2 million personnel files of current and former employees from the United States Office of Personnel Management in one of the largest government breaches in the nation’s history.

Files included 21.5 million security clearance background investigations and 5.6 million fingerprints.

2015

A large insurance company reports a breach of their systems in which the personal information of 78.8 million current and former customers is stolen. (That’s roughly the population of California, Illinois, New York and Maryland combined.)

2015

Lockerpin malware is discovered. It is considered the first ransomware able to permanently lock Android smartphones or tablets by resetting a user’s PIN.

2015

A large insurance company reports a breach of their systems in which the personal information of 78.8 million current and former customers is stolen. (That’s roughly the population of California, Illinois, New York and Maryland combined.)

2015

Files included 21.5 million security clearance background investigations and 5.6 million fingerprints.
Emails from the Democratic National Committee are leaked to WikiLeaks in the run up to the 2016 United States presidential election. According to the DNC, Russian intelligence group Cozy Bear infiltrated the DNC network as far back as 2015, nearly a year before the leaks of the pilfered material began. A second Russian group - Fancy Bear, hacked the DNC’s systems in 2016. The DNC wouldn’t notice the presence of either until April 28, 2016, at which point it called in a security firm to help analyze and mitigate the damage.¹

The WannaCry worm infects over 230 thousand computers in more than 150 countries within 24 hours. It is the largest ransomware offensive to date, and is the first ransomware delivered by worm, a self-replicating and distributing malware. WannaCry targeted a vulnerability in older operating systems.²

OPTIV HISTORY

February 2017: Optiv completed a majority stake equity transaction with KKR, enabling acceleration of service and solutions capabilities and global expansion.

Sources:
1 www.cybersecurityventures.com/cybersecurity-ceo-the-history-of-cybercrime-from-1834-to-present/ ; 2019
2 www.varonis.com/blog/events-that-changed-cybersecurity/ ; 2020
One of the largest consumer credit bureaus is hacked, exposing the data of 143 million users, including their Social Security numbers, birth dates, addresses, driver’s license numbers and, in some cases, credit card numbers. This leads to the resignation of their CEO.1

How did this happen?

Initially hacked via a consumer complaint web portal. A widely known vulnerability that should have been patched but, due to failures in internal processes, wasn’t.2

The attackers moved to other servers because the systems weren’t adequately segmented, where they found plain text usernames and passwords allowing access to further systems.2

Data was pulled out of the network undetected for months because the credit bureau failed to renew an encryption certificate.2

The company did not publicize the breach until more than a month after they discovered it had happened.2

Sources:
1 www.varonis.com/blog/events-that-changed-cybersecurity/; 2020
2 www.cybersecurityventures.com/cybersecurity-the-history-of-cybercrime-from-1834-to-present/; 2019
Cisco Talos researchers discover 74 Facebook groups dedicated to cybercrime, including the sale of stolen credit card information and identities, spam lists and hacking tools. After pressure from Cisco, Facebook deleted these groups, though new ones continue to appear.\(^1\)

**2017**

**Taco Hack**

Eastern European cybercriminals use phishing techniques to steal the credit card information of millions of Chipotle customers.\(^1\)

**2019**

**BUSTED**

Cisco Talos researchers discover 74 Facebook groups dedicated to cybercrime, including the sale of stolen credit card information and identities, spam lists and hacking tools. After pressure from Cisco, Facebook deleted these groups, though new ones continue to appear.\(^1\)

The United States Federal Bureau of Investigation (FBI) notifies Citrix that cybercriminals had likely accessed the company’s internal network through the use of “password spraying”, a brute force technique where hackers use common passwords to attempt to access a large number of employee accounts.\(^1\)

**OPTIV HISTORY**

**September 2018:** Optiv launches integrated services portfolios.

**July 2019:** Optiv establishes availability of Advanced Fusion Center solutions designed to enable organizations to accelerate cybersecurity maturity and improve operational outcomes.
It’s hard to talk about 2020 without mentioning the Coronavirus Pandemic.

- **12/31/2019** A pneumonia case of unknown cause in Wuhan, China is reported to the WHO.
- **1/7/2020** Chinese researchers identify a novel coronavirus, later named COVID-19.
- **1/9/2020** First reported death from COVID-19.
- **1/21/2020** First reported case in the US.
- **1/30/2020** COVID-19 outbreak is declared a public health emergency of international concern.
- **2/15/2020** First recorded COVID-19 death in the US.
- **2/29/2020** COVID-19 case count tops 1 million.
- **4/4/2020** New Zealand’s prime minister, Jacinda Ardern, says that government will lift all COVID-19 restrictions except border controls almost immediately after report of zero cases in the country.
- **5/1/2020** Macy’s announces they will reopen 68 stores in states which have lifted restrictions. With state and local approval and improvement in COVID-19 rates, they plan to reopen the rest of their 775 stores by mid-June.
- **6/1/2020** Colorado health officials announce they expect a bigger second wave of Coronavirus than the first.
Microsoft warns hospitals about the risks of ransomware attacks due to insecure VPN devices and gateways.\(^5\)

Fake Zoom installers being used to distribute malware are discovered.\(^7\)

Google blocks 18 million COVID-related malware and phishing emails per day over the previous week.\(^8\)

Several phishing campaigns are discovered leveraging the Family and Medical Leave Act, small business disaster relief funds and parcel delivery services to deliver malware.\(^9\)

United States and United Kingdom security agencies identify hacking campaigns by advanced persistent threats targeting healthcare and medical researchers fighting the coronavirus.\(^10\)

The gap between cybersecurity risk and defensive effectiveness is as wide as it’s ever been for most companies.\(^11\)

Fraudsters use COVID-19 to target younger generations.\(^12\)

The Global Cybersecurity Market Assessment for 2020 predicts growth deviations due to COVID-19 and places the market at $230 Billion in 2021.\(^13\)

Sources:
1. ZDNet
2. WHO, Rolling updates on coronavirus disease (COVID-19)
3. Business Insider
4. FBI.gov
5. Microsoft
6. Forbes
7. Bleeping Computer
8. Talos Intelligence
9. Securityintelligence.com
10. CISA
11. Forbes
12. Security Magazine
13. Business Insider
Working from Home Shift

2020

“Home is the new enterprise” – Dave Dewalt

OPTIV HISTORY
April 2020: Kevin Lynch is named as CEO of Optiv

56%
An estimated 56% of employees in the United States are in a role that is at least somewhat compatible with working remotely.

3.6%
As of 2018, 3.6% of the United States workforce, some 5 million people, work from home half of the time or more. According to a 2016 Gallup poll, 43% of employees work from home at least some of the time. We predict that the longer people are required to work from home, the more widespread its adoption will be in the long term.

“A typical employer can save about $11 thousand/year for every person who works remotely half of the time.”
Kate Lister, President Of Global Workplace Analytics

Sources:
www.news.gallup.com/poll/306695/workers-discovering-affinity-remote-work.aspx

PREDICTION
Based on historical trends, employees who worked remotely before the pandemic will do so more often once offices reopen. We also predict that significant numbers of those who had never worked remotely before the pandemic will continue to work from home in some capacity. We estimate that 25-30% of the workforce will work from home multiple days per week by the end of 2021.

American’s Increasingly Working Remotely

March 13-15

March 3-April 2

March 3-April 2
Top Six Cybersecurity Trends for 2020

1. **75-80% of the United States workforce now works from home.** Remote work increases pressure on securing your environment.

2. **Apple’s much-talked-about “privacy as a human right” campaign should cause others to follow.**

3. **We may see the first cases of deepfakes being used to manipulate stock prices.**

4. **Election misinformation campaigns are expected to proliferate.**

5. **Anticipate widespread realignment of IT and security organizations.**

6. **The basics are expected to continue vexing consumers as well as enterprise organizations.**

Sources:
If the trajectory of our past indicates anything, it's that we can expect a wild ride ahead. The rapid pace of innovation in threats, technologies and services have informed these predictions of what we can expect in our near future.
Email will continue to be one of the most attractive systems targeted by attackers through phishing and other techniques to steal credentials, implant malware and encourage wire transfer fraud.

The very first email was sent in 1971, today 250B emails are sent each day.

More than 55% of companies in 2019 fell victim to at least one successful phishing attack.

66% of malware is installed via malicious email attachments.

Impacts of Successful Phishing Attacks

Sources:
1 www.atmail.com/blog/10-email-facts-to-impress/ - 2018
2 Proofpoint 2020 State of the Phish Report - 2020
3 www.varonis.com/blog/cybersecurity-statistics/ - 2020
Ransomware: Computing Gets Personal

PREDICTION #1:
It is a matter of time before attacks compromise our critical infrastructure potentially holding entire regions of the country hostage with energy outages. Just look at the impact to cities and towns when their local government gets hit with ransomware.

PREDICTION #2:
There is currently no defense against deep fake videos and people have shown a propensity to believe news that fits their bias. Clearing your name after a deep fake video has gone viral on social media will be extremely difficult, if not impossible, and in many cases the damage will have already been done. Plus, you can never truly remove the deep fake video from the Internet so you will need to defend yourself again and again in the future. Since private companies control social media platforms, the response to removing deep fake videos will be inconsistent and change with the political landscape.

PREDICTION #3:
As technology becomes more and more embedded in medical devices, human organs could be held for ransom. Imagine having to pay bitcoin to maintain the use of your next generation hearing aid or worse, your insurance company may disable the device until you pay your medical bill.

Sources:
Predictions written by Brian Wrozek, Optiv VP, Corporate Security, Risk and Compliance Management and Physical Security
On Cloud Nine

**PREDICTION**

80% of critical enterprise applications will be hosted in the public cloud and continue to compound the security challenge.

Through 2023, at least 99% of cloud security failures will be the customer’s fault.

By 2021, 50% of enterprises will unknowingly and mistakenly have exposed some IaaS storage services, network segments, applications or APIs directly to the public internet.

Cloud assets were involved in 24% of breaches in 2019, and the cloud breach involved a web application server or email server 73% of the time.

Sources:
- Prediction written by Joe Vadakkan
- Gartner 5 Things You Must Absolutely Get Right for Secure IaaS and PaaS; 2020
- Flexera (Rightscale) State of the Cloud Report from 2019 and 2020
Breaches that include mobile devices in the attack campaign will likely continue to increase. The user interface for mobile devices often makes it more challenging to identify phishing and malicious links. In addition, COVID has potentially forced a relaxation of BYOD security policies (but hopefully only temporarily).
MALWARE WILL BE INFUSED WITH AI smarts to adapt to best avoid detection, and change its tactics real-time based on the victim’s unique environment to maximize its impact. AI-enabled malware can start along one attack path then determine a different trajectory would create a higher probability of success.

AI can relieve overburdened security teams by automating key steps of the threat prevention, detection and response process.

52% of companies have security automation at least partially deployed as of 2019.

Breach costs for those organizations with security automation fully deployed were roughly 50% lower than those with no automation program.

Sources:
1 Optiv/ESI Security Executives Survey ; 2020
2 Ponemon Cost of a Data Breach Report ; 2019

Deepfakes will increasingly be used by cyber criminals to steal sensitive information, convince victims to disburse money to them, or manipulate public perception around important issues.

AI CAN BE USED TO DEVELOP “DEEPFAKES” by using freely available video of public figures or influencers and completely altering the words being spoken in a nearly imperceptible way.

The Power of AI

PREDICTION

AI-enabled attacks will rise from the #8 ranked threat today to the #4 ranked threat in just two years.

The Power of AI

PREDICTION

AI-enabled attacks will rise from the #8 ranked threat today to the #4 ranked threat in just two years.

The Power of AI

PREDICTION

AI-enabled attacks will rise from the #8 ranked threat today to the #4 ranked threat in just two years.
These are a few of my favorite IoTs

VROOM VROOM
The number of IoT units built into Automotive and Enterprise solutions will more than double over the next 5 years, from **5.8 billion in 2020** to **12.1 billion in 2025**.

By 2024, at least **50%** of enterprise applications in production will be **IoT-enabled**.

**PREDICTION**

Cyber losses related to connected IoT devices will increase substantially to the 2nd most problematic component of IT infrastructure contributing to cyber loss. IoT is currently seen as the 11th.

Sources:
Prediction written by J.D. Padgett
1. Gartner IoT Forecast as of July, 2020
2. Gartner Predicts 2019: IoT Will Drive Profound Changes to Your Core Business Applications and IT Infrastructure, 2018
SINGULAR FOCUS ON CYBERSECURITY
Our staff is comprised of skilled cybersecurity professionals who eat, sleep and breathe cybersecurity; providing you with unmatched insight and perspective, depth and breadth of services.

END-TO-END CAPABILITIES
We are a leading security solutions integrator (SSI), digging into your existing program, identifying what is working and what’s duplicative, determining what it takes to get your security right and stubbornly effective, and then executing with precision. After we deliver solutions that work, we provide the expertise and offerings to handle as little or as much of the ongoing management burden as you want.

BREADTH OF EXPERIENCE
Our solutions are designed to address your specific business objectives, and drive desired positive outcomes.

WHY OPTIV?

FLEXIBLE CYBERSECURITY MODELS
Our flexible cybersecurity models are intended to help your organization better support continuously evolving business needs. We enable you to optimize and rationalize existing cybersecurity programs so that your organization can evolve in highly effective and integrated ways, and transform how you are procuring, consuming, integrating, implementing and operationalizing cybersecurity.

INSIDE-OUT APPROACH
We start with the core requirement of every enterprise – risk mitigation – and build out from there with individually customized strategy, infrastructure, rationalization, operations optimization and ongoing measurement. This is how you, your organizational leaders and your board can reverse the toxic trends you face today and turn your security operation inside-out.
OUR SERVICES

CYBER DIGITAL TRANSFORMATION

As your trusted digital transformation (DX) partner, Optiv aligns your business objectives with a security-by-design approach, connecting agile processes and controls with emerging security and cloud technologies for a successful digital program. We enable your organization to achieve the flexibility you need to confidently secure, scale and adapt to new emerging trends while delivering any DX initiative.

IDENTITY AND DATA MANAGEMENT

Rather than procuring and implementing siloed solutions, Optiv helps you integrate critical identity and data management (IDM) elements into a comprehensive, flexible solution that is delivered as-a-service, as a managed service, or on-premise. Optiv’s strategic IDM programs allow you to provide the right people access to the right data – in the right manner – maintaining trust and compliance for your business and your customers.

RISK MANAGEMENT

Optiv’s Risk Management and Transformation services align your organization’s security program with business needs to reduce risk. We are the only security solutions integrator that can guide you through an entire security journey, from initial concept and design to program management and optimization, and support all points in between.

SECURITY OPERATIONS

By integrating threat intelligence, risk management profiling, orchestration and automation tools, and advanced and automated analytics applied to ongoing data capture, Optiv has changed cybersecurity operations to be highly scalable, responsive and flexible to your unpredictably shifting business needs.

THREAT MANAGEMENT

Optiv’s threat management approach allows your organization to identify vulnerabilities and malicious activity faster, reduce threat actor dwell time and build security into your infrastructure and applications from the start, enabling a stronger security posture.

INTEGRATION AND INNOVATION

Optiv’s Integration and Innovation services help break down security technology silos to maximize the effectiveness of your organization’s current investments. These services help you expand and custom-build unique solutions to streamline business and cybersecurity challenges.
Optiv is a security solutions integrator – a “one-stop” trusted partner with a singular focus on cybersecurity. Our end-to-end cybersecurity capabilities span risk management and transformation, cyber digital transformation, threat management, security operations, identity and data management, and integration and innovation, helping organizations realize stronger, simpler and more cost efficient cybersecurity programs that support business requirements and outcomes. At Optiv, we are modernizing cybersecurity to enable clients to innovate their consumption models, integrate infrastructure and technology to maximize value, achieve measurable outcomes, and realize complete solutions and business alignment. For more information about Optiv, please visit us at www.optiv.com.

©2020 Optiv Security Inc. All Rights Reserved.