cwpro

An abridged history of information security.

By Rick Howard, CyberWire CSO and Chief Analyst

When I think about our relatively short 50 year infosec history, I can make the case that it roughly coalesces around four phases:

Phase 1 – The mainframe (1960 - 1981)
Phase 2 – The personal computer (1981 - 1995)
Phase 3 – The Internet (1995 - 2006)
Phase 4 – The Cloud (2006 - Present)

It's not a perfect representation but each phase represents a major disruption in how people used computers and consequently, changed how security practitioners thought about securing those computers too.

As we look at the history, certain recurring elements show up at each point.

🏢 **Entities**. Government, commercial and academic organizations that instigated some new idea or program or research, like how Gartner coined the term Cloud Access Service Broker, or CASB, for security technology that protects SaaS applications in 2011.

👹 **Adversary Playbook Names**. Code names assigned to hacker attack sequences across the intrusion kill chain that researchers have noticed repeatedly in the wild like BlackByte (AKA Digital Shadows), an infamous ransomware group.

🔔 **Firsts**. The initial time something happens, like when Aleph One published "Smashing The Stack For Fun And Profit" in 1996, the first published document about the practice of buffer overflow attacks against software.

📚 **Papers and Books**. Written research that invented new things like how Dr. Dorothy Denning published her paper, "An Intrusion Detection Model," in 1986 leading the way for the first commercial Intrusion Detection tools.

👫 **People**. The humans behind the great infosec ideas like how Dr. Fred Cohen published the first papers in the early 1990s that used Defense-in-Depth to describe a common cyber defense architecture model.

🗡️ **Law and Standards**. The legislation that governments passed to control activity in cyberspace like the European Parliament's General Data Protection Regulation, a legal framework that requires businesses to protect the personal data and privacy of European Union citizens.

🔑 **Technologies**. A term of art referring to an application of knowledge for practical ends like passwords or two-factor-authentication.

🧰 **Tools**. A hardware / software device that accomplishes some cybersecurity function, such as a Firewall.

📌 **Strategy and Tactics**. Strategy is the action plan that takes you where you want to go, like zero trust, and tactics are the individual steps that will get you there, like identity and authorization management systems.

Prehistory (prior to 1960)

1824 — The Prussian Army 🏢 adopted a wargaming genre called Kriegsspiel 🧰 (literally “wargame” in German). Blue game pieces represented the Prussian Army (the color of their uniforms). Red blocks represented the enemy forces. Network defenders adopted this model in Red Team / Blue Team / Purple Team operations 🔑 in the 2000s.[69]

1945 — Dr. Stanislaw Ulam 👫, Dr. John von Neumann 👫, and Dr. Nicholas Metropolis 👫 built the first Monte Carlo Simulations 🔑 while working to create the atomic bomb at Los Alamos during WWII.[49]

Phase 1 – The Mainframe (1960 - 1981)

1960 — Dr. Fernando Corbató 👫 introduced the idea of using passwords 🔑 to keep users on the same mainframe out of each other’s files. Also, it provided a way to limit each user’s time (the initial max was four hours.)[1, 2]

1960 — John Draper 👫 and other phone phreakers (the first hackers) 👫, became famous for using toy whistles 🧰 found in Cap’n Crunch cereal boxes and other home made devices, that emitted a tone at 2600Hz, the exact sound that could seize a dial tone from an AT&T 🏢 pay phone and allowed phone phreakers 👫 to make free phone calls.[73]

1967 — Dr. Willis Ware 👫 published "The Ware Report" 📚 to the Defense Science Board for ARPA 🏢 that led to the first formal penetration testing 🔑 efforts and to the development of the US Government's publication of the "Rainbow Series" 📚 of publications.[67]

1969 — UCLA 🏢 and the Stanford Research Institute 🏢 established the first internet connection. According to Andrew Blum 👫, in the book "Tubes: A Journey to the Center of the Internet” 📚, “The internet took in its first breath.”[76]

1972 — James P. Anderson 👫, in a report to the Electronics System Division of the US Air Force 🏢, outlined a series of definitive steps that tiger teams (Penetration Test Teams 🔑) could take to test systems for their ability to be penetrated and compromised.[66]

1974 — The US Air Force 🏢 conducted the probably first penetration test 🔑 of its Multics operating system.[66]

Key

🔑 Technologies 🧰 Tools 🖋️ Law/Standards 👹 Adversary Playbooks
🏢 Entities 🔔 Firsts 📌 Strategy/Tactics 📚 Papers/Books 👫 People

1976

Edward Luttwak 👫 published his book, “The Grand Strategy of the Roman Empire from the First Century AD to the Third” 📚, in which he coined the phrase “Defense-in-Depth” to describe his controversial theory about the Roman Army’s defensive posture from the first to third century A.D.[3, 4]

1977

Wulf 👫, Cohen 👫, Corwin 👫, Jones 👫, Levin 👫, Pierson 👫, and Pollack 👫 introduced the idea of virtual machines 🔑 (Virtual Sandboxes 🔑) for their Carnegie Mellon University 🏢 Hydra system 🧰.[5]

1978

Gary Thuerk 👫, a marketing manager, sent the first unsolicited bulk email (SPAM 🔑) to roughly 400 prospects via ARPANET🔑, a forerunner to the modern internet, and reaped $13 million in sales for his company.[59]

1978

Ward Christensen 👫 and Randy Suess 👫 established the first dial-up bulletin board system 🧰 in Chicago during a blizzard because they wanted a way to keep up with their computer club without having to gather together in person.[78]

1979

Unix V7 🧰 introduced the chroot system 🔑; changing the root directory of a process and its children to a new location in the filesystem. This was the beginning of process isolation 📌: segregating file access for each process, the next step in virtual machines 🔑.[6]

1980

Leaders 👫 from the US Nuclear Regulatory Commission 🏢 published their guidance on protecting nuclear power plants built before 1979. They advocate for a Defense-in-Depth 📌 model.[3, 102]

1980

James Anderson 👫 publishes "Computer Security Threat Monitoring and Surveillance" 📚, the first research on intrusion detection 🔑.[68]

Phase 2 – The PC (1981 - 1995)

1981

IBM 🏢 unveiled the company's entrant into the nascent personal computer market, the IBM PC 🧰, and started the second phase of infosec history. Other companies, including Apple 🏢 and Tandy Corp 🏢, were already making personal computers, but no other machine carried the revered IBM name.[75]

1983

The US Government 🏢 published the first book in the series of Rainbow Books 📌, “The Orange Book: DOD Trusted Computer System Evaluation Criteria” 📚.[8]

Key

🔑 Technologies 🧰 Tools 🔪 Law/Standards 👹 Adversary Playbooks
🏢 Entities 🔔 Firsts 📌 Strategy/Tactics 📚 Papers/Books 👫 People

1983

Steve Capps 👫 created the first fuzzer 🔑 program by repurposing another tool called “The Monkey” 🧰, where a Macintosh computer could demo itself by playing back recorded actions, to create random mouse clicks and keyboard input in order to test the MacWrite and MacPaint applications. The term “fuzzer” 🔑 did not come for another seven years but the technique has been widely used since by researchers trying to find software vulnerabilities 🔑.[61]

1984

Dr. Dorothy Denning 👫, while working for SRI International 🏢, helped to develop the first model for intrusion detection 🔑, the Intrusion Detection Expert System (IDES) 🧰, which provided the foundation for the IDS technology 🔑 development that was soon to follow.[7]

1984

Eric Corley 👫 (AKA Emmanuel Goldstein 👫 – the shadowy leader of the resistance in George Orwell’s “1984” 📚) founded “2600: The Hacker Quarterly” 📚, an American magazine (sometimes called “the hacker’s bible” 📚) that discussed issues around legal, ethical, and technical debates over hacking 🔑.[72]

1986

Dr. Dorothy Denning 👫 published her paper, "An Intrusion Detection Model" 📚, in the proceedings of the Seventh IEEE Symposium on Security and Privacy leading the way for the first commercial Intrusion Detection tools 🧰. Her paper is the basis for most of the work in IDS technology 🔑 that followed.[9]

1986

The US Congress 🏢 passed The Computer Fraud and Abuse Act (CFAA) 🖋️ as an amendment to the first federal computer fraud law to prohibit intentionally accessing a computer (hacking 🔑) without authorization with harsh penalty schemes.[70]

1986

The US Congress 🏢 passed the Electronic Communications Privacy Act (“ECPA”) 🖋️ to promote “the privacy 🔑 expectations of citizens and the legitimate needs of law enforcement.”[71]

1987

Bernd Fix 👫 discovered a method to neutralize the Vienna virus 🧰, becoming the first documented antivirus software 🔑 ever written.[10]

1987

Omni magazine 🏢 coined the word “cyberwar” 🔑 and defined it in terms of giant robots and autonomous weapon.[74]

1988

Dr. Clifford Stoll 👫 publishes “STALKING THE WILY HACKER” 📚 that outlines the first ever public cyber espionage campaign 🔑 sponsored by Russia 🏢 using East German hacker mercenaries that targeted US governmental agencies. The next year, Stoll 👫 published his book “The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage” 📚 that covered the same material with more detail.[47, 48]

Key

🔑 Technologies 🧰 Tools 🖋️ Law/Standards 👹 Adversary Playbooks
🏢 Entities 🔔 Firsts 📌 Strategy/Tactics 📚 Papers/Books 👫 People

1988	Jeff Mogul 👫, Brian Reid 👫, and Paul Vixie 👫 working for Digital Equipment Corp 🏢 conducted the first research on firewall technology 🔑 with the gatekeeper.dec.com gateway 🧰 and “ScreeND" 🧰 tools. This was the first generation of firewall architectures 🔑.[11]
1988	Robert Tappan Morris 👫, a first-year computer science graduate student at Cornell 🏢 , created and launched the “Morris Worm” 🧰 onto the internet; the first of its kind to cause as much damage as it did (10% of the existing internet affected). It also resulted in the first felony conviction in the US under the 1986 Computer Fraud and Abuse Act 🖋️ and prompted DARPA 🏢 to fund the establishment of the CERT/CC 🏢 at Carnegie Mellon University 🏢 .[44, 45, 46]
1988	The Kerberos v4 protocol 🧰 was first publicly described in a Usenex conference paper, a network security protocol that authenticates 🔑 service requests between two or more trusted hosts across an untrusted network.[53]
1988	University of Wisconsin’s 🏢 Professor Barton Miller 👫 coined the phrase “fuzz test” 🔑 in “An empirical study of the reliability of UNIX utilities” 📚, the technique has been widely used since by researchers trying to find software vulnerabilities 🔑.[62]
1989	The developers 👫 from The Haystack project 🔑 formed the commercial company, Haystack Labs 🏢, and released the last generation of the technology, Stalker 🧰, a host-based, pattern matching system that included robust search capabilities to manually and automatically query the audit data."[102]
1989	John Romkey 👫 created the first Internet of Things (IoT) 🔑 device; a toaster that could be turned on and off over the Internet, at the '89 INTEROP conference🔑.[30]
1989	Dave Presotto 👫 and Howard Trickey 👫 of AT&T Bell Laboratories 🏢 pioneered the second generation of firewall architectures 🔑 with their research in circuit relays 🔑, which are also known as circuit level firewalls 🔑. They also implemented the first working model of the third generation of firewall architectures 🔑, known as application layer firewalls 🔑. However, they neither published any papers describing this architecture nor released a product based upon their work.[11, 12]
1990	Third generation of firewall architectures 🔑 was independently researched and developed by Gene Spafford 👫 of Purdue University 🏢, Bill Cheswick 👫 of AT&T Bell Laboratories 🏢, and Marcus Ranum 👫 describing application layer firewalls 🔑.[11, 12]
1990	The Chinese 🏢 tell a group of North Korean 🏢 hackers 👫 that they could use the Internet to steal secrets and attack the government’s enemies.[52]

Key

🔑 Technologies 🧰 Tools 🖋️ Law/Standards 👹 Adversary Playbooks
🏢 Entities 🔔 Firsts 📌 Strategy/Tactics 📚 Papers/Books 👫 People

1991 Marcus Ranum's 👫 firewall 🔑 work received the most attention and took the form of bastion hosts 🧰 running proxy services 🧰.[12]

1991 Dr. Fred Cohen 👫 published the first papers in 1991 and 1992 that used Defense-in-Depth 📌 to describe a common cybersecurity model in the network defender industry.[13, 14, 104]

1992 Digital Equipment Corp 🏢 shipped DEC SEAL 🧰, the first commercial firewall and included proxies developed by Marcus Ranum👫.[11]

1993 Jon Arquilla 👫 and David Ronfeldt 👫, working for the RAND Corporation 🏢, published “Cyberwar Is Coming!” 📚, introducing the idea that cyber attacks could be used for traditional warfare.[43]

1993 Tim Howes 👫, Steve Kille 👫, and Wengyik Yeong 👫 develop the Lightweight directory access protocol (LDAP) 🧰, a open source application protocol to manage authentication 🔑 access to usernames, passwords, email addresses, printer connections, and other static data within directories. This protocol will be an important piece to Microsoft’s 🏢 Active Directory 🧰.[54]

1993 Jeff Moss (AKA Dark Tangent) 👫 organized the first DEFCON security conference 🔑 that caters to the Hacker 👫 ethos.[88]

1994 William Cheswick 👫 and Steven Bellovin 👫, published “Firewalls and Internet Security: Repelling the Wily Hacker” 📚, the first book on firewalls 🔑 as a technology. They called it a circuit-level gateway 🔑 and packet filtering 🔑 technology.[103]

1994 Check Point Software 🏢 released the first stateful inspection 🔑 commercial firewall.[12]

1994 Amazon 🏢 began work on an e-commerce service called Merchant.com 🧰 to help third-party merchants like Target or Marks & Spencer build online shopping sites on top of Amazon’s e-commerce engine. This eventually led to AWS 🧰.[15, 16]

1994 Vladimir Levin 👫 successfully hacked Citibank 🏢 to the tune of $10 million that is likely the first significant cyber crime.[89]

Phase 3 – The Internet (1995 - 2006)

1995 The internet 🧰 and the World Wide Web 🧰 became a mainstream phenomena.[77]

Key

🔑 Technologies 🧰 Tools 🖋️ Law/Standards 👹 Adversary Playbooks
🏢 Entities 🔔 Firsts 📌 Strategy/Tactics 📚 Papers/Books 👫 People

1995	Citicorp 🏢 hired Steve Katz 👫 to be the first Chief Information Security Officer 🔑.[90]
1996	Aleph One 👫 published “Smashing The Stack For Fun And Profit” 📚, the first published document about the practice of buffer overflow attacks 🔑 against software.[37]
1996	The US Congress 🏢 passed the Health Insurance Portability and Accountability Act (HIPAA) 🖋️ to require the adoption of national standards for electronic health care transactions and code sets, as well as unique health identifiers for providers, health insurance plans and employers.[83]
1997	Deputy Secretary of Defense John Hamre 👫, during a congressional hearing, said that the United States must prepare for an “electronic Pearl Harbor” 🔑, a calamitous, surprise cyberattack designed not just to take out military command-and-control communications but to physically devastate American infrastructure.[74]
1997	This NSA 🏢 Red Team 🔑 conducted a no-notice Vulnerability Assessment/ Penetration Test (Code name: Eligible Receiver 🧰) of critical government networks to include the DoD. The report showed the network was so poorly protected the results were quickly classified.[100]
1998	Hactivist group 🔑 “Cult of the Dead Cow” 👹 released the first version of Back Orifice 🧰, authored by Sir Dystic 👫, at DEFCON 6 🔑 to demonstrate the lack of security in Microsoft's Windows 9x series of operating systems.[94]
1998	The Defense Information Systems Agency 🏢 discovered Russian 🏢 hacker 👫 activity against the Pentagon 🏢, National Aeronautics and Space Administration (NASA) 🏢, and some affiliated academic and laboratory facilities 🏢 (Code name: Moonlight Maze 👹). The hackers 👫 stole unclassified information on contracts, research, military data, troop data, and maps of military installations.[100]
1999	David Baker 👫, Steven Christey 👫, William Hill 👫, and David Mann 👫, working for MITRE 🏢, published "The Development of a Common Enumeration of Vulnerabilities and Exposures" 📚, the establishment of the first public Common Vulnerability Enumeration (CVE) 🔑 database.[39]
1999	Kevin Ashton 👫 coined the term “the internet of things” 🔑 at a Procter & Gamble 🏢 conference.[31]
1999	The US Congress 🏢 passed the Gramm-Leach-Bliley Act (GLBA) 🖋️ to protect consumers' personal financial information held by financial institutions.[86]

Key

🔑 Technologies 🧰 Tools 🖋️ Law/Standards 👹 Adversary Playbooks
🏢 Entities 🔔 Firsts 📌 Strategy/Tactics 📚 Papers/Books 👫 People

1999	Qiao Liang 👫 and Wang Xiangsui 👫, two Chinese colonels, publish “Unrestricted Warfare: China’s Master Plan to Destroy America” 📚, that proposes the strategy of what will become to be known as asymmetric warfare 📌 to level the playing field against the US military might.[95, 96]
2000	Poul-Henning Kamp 👫 introduced Jails 🧰 that allowed administrators to partition a FreeBSD Unix 🧰 computer system into several independent, smaller systems – called “jails” 🧰 – with the ability to assign an IP address for each system and configuration; the next step in virtual machines 🔑.[6]
2000	Internet founding father Vint Cerf 👫 coined the phrase cyber hygiene 📌 when he testified to the United States Congress Joint Economic Committee. INfosec practitioners had been executing this best practice for at least a decade proper, but Vint Cerf 👫 gave it a name.[17]
2000	Microsoft 🏢 released Windows Server 2000 🧰, the first release of Active Directory 🧰 which became the de facto Identity and Access Management 🔑 system for most organizations.[54]
2001	17 software developers publish the “Agile Manifesto” 📚, a rejection of the Waterfall model 🧰 and an embracement of the idea of producing real, working code as a milestone of progress. This is the start of the Agile 📌 software development movement and the precursor to DevOps 📌 and DevSecOps 📌.[64]
2001	The Payment Card Industry Security Standards Council 🏢 established the Payment Card Industry Data Security Standard (PCI DSS) 🗡️, cybersecurity controls and business practices that any company that accepts credit card payments must implement.[84]
2002	Security Assertion Markup Language (SAML) V1.0 🧰 became an OASIS 🏢 standard, an open source standard that allows identity 🔑 providers to pass authorization 🔑 credentials to service providers. OASIS 🏢 is a non-profit standards body.[56]
2002	Bill Gates 👫 turns Microsoft 🏢 on a dime to implement "Trustworthy Computing" 📌, shuts down Windows development for the first time ever to get a handle on the security issues the products were facing, and creates the Microsoft Security Development Lifecycle (SDL) 🔑.[65]
2002	The US Congress 🏢 passed the Federal Information Security Management Act 🗡️ that requires federal agencies to implement a program to provide security for their information and information systems.[81]

Key

🔑 Technologies 🧰 Tools 🗡️ Law/Standards 👹 Adversary Playbooks
🏢 Entities 🔔 Firsts 📌 Strategy/Tactics 📚 Papers/Books 👫 People

2002	The US Congress 🏢 passed the Sarbanes-Oxley Act 🗡️ to protect investors and the public by increasing the accuracy and reliability of corporate disclosures and holds companies liable for bad Identity and Access Management 🔑.[55, 85]
2003	Amazon 🏢 installs infrastructure-as-code 🔑 internally (the beginnings of DevOps 📌); a set of common infrastructure services everyone could access without reinventing the wheel every time. Business leaders realized that they could build the operating system for the internet from these services. This eventually led to AWS 🧰.[15, 16]
2003	Dave Wickers👫 and Jeff Williams👫, working for Aspect Security 🏢, a software consultancy company, published an education piece in 2003 on the top software security coding issues of the day. That eventually turned into the OWASP Top 10 🧰, a reference document describing the most critical security concerns for web applications.[91]
2003	The US Department of Defense 🏢 discovers the first Chinese 🏢 computer cyber espionage 🔑 operation codenamed “Titan Rain" 🔔.[97]
2004	Google 🏢 invents Site Reliability Engineering (SRE) 🔑, the first foray into infrastructure as code 🔑 (the beginnings of DevOps).[18]
2004	VoIP service provider BroadVoice 🏢 introduced the idea of Bring Your Own Device (BYOD) 🔑 to work.[29]
2005	Concur 🏢 becomes the first company to offer a SaaS Cloud Platform 🔑.[19]
2005	Brad Fitzpatrick 👫 develops the first generation OpenID 🧰 authentication 🔑 protocol. This eventually becomes the authentication 🔑 layer for OAuth 🧰.[57]
2005	Gartner 🏢 security analysts Mark Nicolett 👫 and Amrit Williams 👫 coined the term SIEM (Security Event and Information Management) 🔑 as an improvement to traditional log collection 🔑 systems to offer long term storage, combined log analytics, with a focus on security events.[60]

Phase 4 – The Cloud (2006 - Present)

2006	Amazon 🏢 becomes the first Company to offer an IaaS Cloud Platform 🔑 (Amazon Elastic Compute or AWS 🧰).[15, 16]
2006	First managed identity 🔑 services.[55]

Key

🔑 Technologies 🧰 Tools 🗡️ Law/Standards 👹 Adversary Playbooks
🏢 Entities 🔔 Firsts 📌 Strategy/Tactics 📚 Papers/Books 👫 People

2007	Palo Alto Networks 🏢 launched the first next generation firewall 🔑, a firewall that not only does stateful inspection at layer 3, but more importantly, allows rules at the application layer, layer 7.[21]
2007	Russian 🏢 launched DDOS attacks 🧰 against Estonia 🏢.[74]
2008	According to Cisco Internet Business Solutions Group (IBSG) 🏢, the Internet of Things (IoT) 🔑 became real when more “things or objects” were connected to the Internet than people.[30]
2008	Russian 🏢 Hackers 👫 (Turla 👹, Snake 👹, APT 28 👹) penetrated the Pentagon’s classified networks. The Pentagon 🏢 deployed the fix, code name Operation Buckshot Yankee 📌 later that day. This event led to the creation of what has become Cyber Command 🏢.[52]
2008	Dr. Gary McGraw 👫 published the first Building Security In Maturity Model (BSIMM) 🧰 report; a survey of some 30+ companies that collated initiatives and activities around software security.[92]
2008	The Chinese People’s Liberation Army (PLA) 🏢 penetrated Lockheed Martin’s 🏢 networks and stole the plans related to the F-35, the world’s most sophisticated, and certainly most expensive, fighter jet.[97]
2009	Intel 🏢 is probably the first commercial company to approve a formal Bring Your Own Device (BYOD) 🔑 policy when the company realized that many of its employees were bringing their own devices into work and connecting to the corporate network.[29]
2009	Pravir Chandra 👫 published the first SAMM (Software Assurance Maturity Model) 🧰; a prescriptive security model that gives practitioners a way to measure how well they’re doing against a set of prescribed best practices.[92]
2009	Robert Gates 👫, President Obama’s secretary of defense, concluded after the Russian 🏢 (Turla 👹, Snake 👹, APT 28 👹) penetration of the Pentagon’s classified networks in 2008 to create the US Cyber Command 🏢 to direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners.[52, 101]
2010	Lockheed Martin’s 🏢 Hutchins 👫, Cloppert 👫, and Amin 👫 publish “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains" 📚, the origination of the intrusion kill chain 🔑 strategy.[22]

Key

🔑 Technologies 🧰 Tools 🔪 Law/Standards 👹 Adversary Playbooks
🏢 Entities 🔔 Firsts 📌 Strategy/Tactics 📚 Papers/Books 👫 People

2010	John Kindervag 👫, working for Forrester🏢, published “No More Chewy Centers: Introducing The Zero Trust Model Of Information Security” 📚. The idea of zero trust 🔑 had been around for a number of years but this paper solidified the concept.[23]
2010	The Industrial Control Systems CERT 🏢 starts tracking Industrial Control Systems 🧰 vulnerabilities.[32]
2010	The US and Israeli governments 🏢 launched “Olympic Games” 🔔, the first public cyber attack (Stuxnet 🧰) to destroy another country’s critical infrastructure; in this case, the Iranian 🏢 uranium enrichment plant at Natanz. This might be the first public cyber attack to crossover from cyber espionage 🔑 to cyber warfare 🔑.[50, 51, 52]
2010	First Identity as a Service 🧰 in the cloud.[55]
2010	The Internet Engineering Task Force (IETF) 🏢 released OAuth 🧰 as an open-standard (RFC 5849 🖋️) authorization 🔑 protocol that describes how unrelated servers and services can safely delegate authenticated 🔑 access to their assets without actually sharing credentials.[58]
2010	Google 🏢 publicly announced it had been hacked by the Chinese government 🏢 in what became to be known as Operation Aurora 👹. Before, no commercial company would ever admit such a breach for fear of reputation damage. After, and aided by public disclosure laws, more and more companies follow the practice. The event also led to Google Site Reliability Engineers 👫 rebuilding the Google 🏢 internal network from the ground up using Software Defined Perimeter 🔑 and Zero Trust 🔑 as their main strategies.[97]
2010	The Iranian Government 🏢 announced the creation of a cybercorps 🔑; their answer to counter the US Cyber Command 🏢.[52]
2011	Gartner 🏢 coined the term CASB (Cloud Access Service Broker) 🔑 for security technology that protects SaaS applications 🔑.[24]
2011	Sergio Caltagirone 👫, Andrew Pendergast 👫, and Christopher Betz 👫, working for the US Department of Defense 🏢, published "The Diamond Model of Intrusion Analysis” 📚, written around the same time that the Lockheed Martin 🏢 research team published their intrusion kill chain model 🔑. The authors designed the Diamond model 🔑 specifically for intelligence analysts to track adversary groups across the intrusion kill chain 🔑.[40]

Key

🔑 Technologies 🧰 Tools 🖋️ Law/Standards 👹 Adversary Playbooks
🏢 Entities 🔔 Firsts 📌 Strategy/Tactics 📚 Papers/Books 👫 People

2011	The World Economic Forum 🏢 coined the term Resilience 🔑 "… the ability of systems and organizations to withstand cyber events …"[25]
2011	The US Office of Management and Budget (OMB) 🏢 established The Federal Risk and Authorization Management Program (FedRAMP) 🗡️ to empower federal agencies to use modern cloud technologies, with an emphasis on security and protection of federal information.[82]
2011	The Chinese People's Liberation Army 🏢 hacked RSA 🏢 and stole their secret cryptographic keys responsible for the encryption function of their SecurID tokens 🧰 product line that many organizations used for two factor authentication. It was the first public supply chain attack 🔑 and led to the compromise of Lockheed Martin 🏢, Northrop Grumman 🏢, and L3 🏢. It was also the first time that a pure play commercial company (not a government contractor) noticed adversary lateral movement 🔑 as a step in the hacking sequence; a step that had been captured by the Lockheed Martin's 🏢 intrusion kill chain 🔑 strategy a year before.[98]
2011	Responding to the US 🏢/ Israeli 🏢 operation Olympic Games 🔔, Iranian 🏢 hackers 👫 began DDOSing 🔑 roughly four dozen American financial institutions—including JPMorgan Chase 🏢, Bank of America 🏢, Capital One 🏢, PNC Bank 🏢, and the New York Stock Exchange 🏢.[52]
2012	Iranian 🏢 hackers👫 cripple Saudi Aramco 🏢, the world's largest oil producer, destroying: 30,000 computers and 10,000 servers.[52]
2013	Docker 🏢 released an open source container management platform 🔑 called dotCloud 🧰 and established a partnership with Red Hat Linux 🏢. The idea of containers 🔑 had been around for a while, but this started the momentum to make them standard practice.[20]
2013	Gartner's 🏢 Anton Chuvakin 👫 coined the term Endpoint Threat Detection and Response (ETDR) 🔑, now commonly referred to as EDR (Endpoint Detection and Response) 🔑.[26]
2013	Mandiant 🏢 published "APT1: Exposing One of China's Cyber Espionage Units" 📚, the first public document that outlined the Chinese government cyber attack campaigns across the intrusion kill chain 🔑. Also, the first time the general public starts to notice Cyber Threat Intelligence 🔑 as something infosec professionals do.[38]
2013	MITRE 🏢 established the ATT&CK Framework 🧰, an extension of the intrusion kill chain model 🔑 that operationalized the Lockheed Martin 🏢 strategy document with adversary tactics, techniques, and procedures 🔑.[41]

Key

🔑 Technologies 🧰 Tools 🗡️ Law/Standards 👹 Adversary Playbooks
🏢 Entities 🔔 Firsts 📌 Strategy/Tactics 📚 Papers/Books 👫 People

2013	General Valery Gerasimov 👫, the Chief of the General Staff of the Russian Federation established the unofficial Gerasimov doctrine 🔑 that seeks asymmetric targets (physical and virtual critical infrastructure including space) across the spectrum during war.[74]
2013	Gene Kim 👫, Kevin Behr 👫, and George Spafford 👫 published “The Phoenix Project: A Novel about IT, DevOps, and Helping Your Business Win” 📚 introducing the idea of DevOps 🔑 to the general business world.[93]
2013	Deep Panda 👹 (a Chinese hacking group 🏢) compromised OPM’s 🏢 database containing PII (Personal Identifiable Information) 🔑 on US government clearance holders and might be the largest and most impactful cyber espionage campaign known to the public against any known country. The vast amounts of data collected plus the longevity of it (over 50 years since that’s how long it will take for all individuals caught in the net to age out of government service) will be useful for many years to come.[99]
2013	Iranians 🏢 breach the New York State’s Bowman Avenue Dam’s 🏢 command-and-control system, an example of how nation states could control and damage the critical infrastructure 🔑 of an enemy nation.[52]
2014	Amazon 🏢 became the first Company to offer serverless functions (AWS Lambda 🧰).[27]
2014	The National Institute of Standards and Technology (NIST) 🏢 published the “Framework for Improving Critical Infrastructure Cybersecurity” 📚 that became a cybersecurity best practice maturity model for the community around the ideas of Identify, Protect, Detect, Respond, and Recover 🔑.[42, 87]
2014	US intelligence agencies 🏢 confirm that Russia 🏢 has penetrated the US Electrical Grid 🔑 in many locations using malware called “BlackEnergy” 🧰.[52]
2014	Iranians 🏢 destroy the Sands Casino 🏢 in Las Vegas.[52]
2014	North Korea 🏢 hackers 👫 (Guardians of Peace 👹) crippled Sony 🏢 because of a movie released depicting the North Korean 🏢 Supreme Leader (Kim Jong-un 👫) in an unfavorable light. It marks the first time that a US President, President Obama 👫 , confirmed a cyber attribution 🔑 on national television.[52]
2015	Google 🏢 released Kubernetes 1.0 🧰; an open-source container orchestration system 🔑 and gave it to The Cloud Native Computing Foundation (CNCF) 🏢 to manage.[20]

Key

🔑 Technologies 🧰 Tools 🗡️ Law/Standards 👹 Adversary Playbooks
🏢 Entities 🔔 Firsts 📌 Strategy/Tactics 📚 Papers/Books 👫 People

2015	Security Orchestration 🔑 as an idea emerged.[28]
2016	Six out of every ten companies had a Bring-Your-Own-Device (BYOD)-friendly 📌 policy in place.[29]
2016	The European Parliament 🏢 adopted the General Data Protection Regulation (GDPR) 🖋️, a legal framework that requires businesses to protect the personal data and privacy of European Union (EU) citizens for transactions that occur within EU member states.[79]
2016	North Korean 🏢 hackers 👫 steal $81 Million from the Bangladesh Central Bank 🏢. This marks the first public discovery of a new trend, nations states using government assets to conduct cyber crime for two reasons: APT Side Hustle 🔑 to fund their nation state missions and State Sanctioned Organized Cyber Crime 🔑 to bring revenue into the country.[52]
2017	Gartner 🏢 coined the phrase Security Orchestration and Automation (SOAR) 🔑; tools to orchestrate the security stack.[33]
2017	North Korean 🏢 hackers 👫 launched a ransomware 🔑 attack (code name: WannaCry 👹) using the “Eternal Blue” 🧰 exploit tool in the attack sequence that was stolen from the NSA 🏢 by the Shadow Brokers 👹 hacktivist group 🔑 and made public.[52]
2018	Nir Zuk 👫, the Palo Alto Networks 🏢 founder and CTO, coined the phrase: XDR.[34]
2019	Gartner 🏢 coined the phrase Secure Access Service Edge (SASE) 🔑.[35]
2020	Rick Howard 👫 and Ryan Olson 👫 publish “Implementing Intrusion Kill Chain Strategies by Creating Defensive Campaign Adversary Playbooks” 📚, the next extension to the Intrusion Kill Chain / Diamond / MITRE Attack framework 🔑 models.[36]

Key

🔑 Technologies 🧰 Tools 🖋️ Law/Standards 👹 Adversary Playbooks
🏢 Entities 🔔 Firsts 📌 Strategy/Tactics 📚 Papers/Books 👫 People

References

1. “Man behind the First Computer Password: It’s Become a Nightmare,” by Danny Yadron, The Wall Street Journal, 21 May 2014.

2. “The Guy Who Invented Computer Passwords Thinks They’re a Nightmare,” by Adam Clark Estes, Gizmodo, 22 May 2014.

3. "The Next Board Problem: Automatic Enterprise Security Orchestration – a Radical Change in Direction," by Rick Howard, Palo Alto Networks, 2017.

4. “The Grand Strategy of the Roman Empire from the First Century AD to the Third,” by Edward Luttwak, Published by Johns Hopkins University Press, 1976.

5. “HYDRA -- the Kernel of a Multiprocessor Operating System,” by Wulf, Cohen, Corwin, Jones, Levin, Pierson, and Pollack, ARPA. June 1973.

6. “A Brief History of Containers: From the 1970s till Now,” by Rani Osnat, Aqua Security, 10 January 2020.

7. “The Evolution of Intrusion Detection Systems,” by Paul Innella, Tetrad Digital Integrity, LLC, Symantec, 16 November 2001.

8. “Rainbow Series.” nina.az, 30 October 2021.

9. "An Intrusion Detection Model," Dr. Dorothy Denning, Proceedings of the Seventh IEEE Symposium on Security and Privacy, May 1986, pages 119–131.

10. "Bernd Fix," Computer Hoper, 30 December 2019.

11. “Who Invented the Firewall?” by Kelly Jackson Higgins, Dark Reading, January 15, 2008.

12. “Evolution of the Firewall Industry.” by Cisco Systems, 28 September 2002.

13. “Models of Practical Defenses against Computer Viruses,” by Dr. Fred Cohen, Comput. Secur. 8 (1989): 149-160, 1989.

14. “Defense-in-depth against computer viruses,” by Dr. Fred Cohen, Comput. Secur. 11 (1992): 563-579.

15. “History of AWS,” Javatpoint, 2012.

16. “How AWS Came to Be,” by Ron Miller, TechCrunch, 2 July 2016.

17. "Joint Economic Committee,” United States Congress Joint Economic Committee," 23 February 2000

18. “Site Reliability Engineering: How Google Runs Production Systems,” by Betsy Beyer, Chris Jones, Jennifer Petoff, and Niall Richard Murphy, Published by O’Reilly Media, 16 April 2016.

19. “A SaaS History Lesson – the First SaaS Company’s Exceptional Journey,” by Tomasz Tunguz, Venture Capitalist at Redpoint, 28 April 2015.

20. “The History of Docker’s Climb in the Container Management Market,” by Stefani Muñoz, TechTarget, 2019.

21. “Nir Zuk’s Podcast on Network Security and Upcoming Technology,” by Ankur Shah, Neelima Rustagi, ZeroToExit Podcast,” 2021.

22. "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,” by Eric Hutchins, Michael Cloppert, Rohan Amin, Lockheed Martin Corporation, 2010.

23. "No More Chewy Centers: Introducing The Zero Trust Model Of Information Security," by John Kindervag, Forrester, 2010.

24. “What is a CASB? Cloud Access Security Broker,” McAfee, 2019.

25. "Partnering for Cyber Resilience,” by The World Economic Forum, 2012.

26. “What Is Endpoint Detection and Response? A Definition of Endpoint Detection & Response,” by Nate Lord, Digital Guardian, 23 July 2019.

27. “What Is Serverless? Serverless Computing Explained,” by Josh Fruhlinger, InfoWorld, 15 July 2019.

28. “The Evolution of Security Operations, Automation and Orchestration,” by Jon Oltsik, CSO Online, 9 May 2018.

29. “Is BYOD (Bring Your Own Device) Dead?” by Adam Harkness, NetMotion Software, 21 October 2019.

30. “Internet of Things (IoT) History,” by Trevor Harwood, Postscapes, 12 November 2019.

31. “The IoT History and Future,” by Sandra Khvoynitskaya, 2019.

32. “IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things,” by David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Subodh Gajare, Published by Cisco Press, 13 June 2017.

33. “The Evolution of SOAR Platforms,” by Stan Engelbrecht, SecurityWeek.com, 27 July 2018.

34. “What Is XDR?,” Palo Alto Networks, 2015.

35:“What Is SASE?,” Palo Alto Networks, 2022.

36. "Implementing Intrusion Kill Chain Strategies by Creating Defensive Campaign Adversary Playbooks," by Rick Howard, Ryan Olson, and Deirdre Beard (Editor), The Cyber Defense Review, Fall 2020.

37. "Smashing The Stack For Fun And Profit," by Aleph One, Phrack 49, Volume Seven, Issue Forty-Nine File 14 of 16, 8 November 1996.

38. “APT1: Exposing One of China’s Cyber Espionage Units | Mandiant.” Mandiant.com, 2013.

39. "The Development of a Common Enumeration of Vulnerabilities and Exposures," by David Baker, Steven Christey, William Hill, and David Mann, MITRE, 1999.

40. "The Diamond Model of Intrusion Analysis,” by Sergio Caltagirone, Andrew Pendergast, and Christopher Betz, Center for Cyber Threat Intelligence and Threat Research, Hanover, MD, Technical Report ADA586960, 05 July 2011.

41. "MITRE ATT&CK: Design and Philosophy," by Blake Strom, Andy Applebaum, Doug Miller, Kathryn Nickels, Adam Pennington, and Cody Thomas, MITRE, March 2020.

42. “Framework for Improving Critical Infrastructure Cybersecurity,” by the National Institute of Standards and Technology (NIST), Version 1.0, 12 February 2014

43. “Cyberwar Is Coming!” by Jon Arquilla and David Ronfeldt, RAND Corporation, 1993.

44. “The Day Computer Security Turned Real: The Morris Worm Turns 30,” by Steven Vaughan-Nichols, Senior Contributing Editor, ZDNET, 2 November 2018.

45. “First Indictment under Computer Fraud Act,” Tony Long, WIRED, 26 July 2011.

46. “What Is a CERT, Anyway?” CERT NZ,” 2020.

47. “Stalking The Wily Hacker,” by Clifford Stoll, Communication Of The ACM, vol. 31. No. 5, May 1988.

48. “The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage,” by Clifford Stoll, Published by Gallery Books, 1989.

49. “The Beginning Of The Monte Carlo Method,” by N. Metropolis, Los Alamos Science Special Issue, Vol. 15, 1987, pp. 125-130, 1987.

50. “Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon,” by Kim Zetter, Published by Crown, 3 June 2014.

51. “Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power,” by David E. Sanger, Published by Crown Publishing Group, 1 January 2012.

52. “The Perfect Weapon: How the Cyber Arms Race Set the World Afire,” by David E. Sanger, Published by Crown, 19 June 2018.

53. “Kerberos and Windows Security: History,” by Robert Broeckelmann, Medium, 16 May 2018.

54. “History of LDAP,” by ldapwiki.com.

55:“The Evolution Of IAM (Identity Access Management,)” by SolutionsReview, Youtube, 3 September 2019.

56:“History of SAML,” by saml.xml.org, 2015.

57. “SAML2 vs JWT: Understanding OpenID Connect Part 1,” by Robert Broeckelmann, Medium, 25 March 2017.

58. “What is OAuth? How the open authorization framework works,” by Roger A. Grimes and Josh Fruhlinger, CSO, 20 September 2019.

59. “40 Years on from the First Spam Email, What Have We Learned? Here Are 5 Things You Should Know about Junk Mail,” by Rob Smith, World Economic Forum, 4 May 2018.

60. “The Evolution of SIEM,” by Christian Wiens, Security Boulevard, 13 October 2020.

61. “History: what is fuzzing?” fuzzing.info, 6 May 2012.

62. “An empirical study of the reliability of UNIX utilities,” Barton Miller, Louis Fredriksen, and Bryan So, Communications of the ACM, Volume 33, pp 32–44, 12 December 1990

63. “Celebrating 20 Years of Trustworthy Computing,” by Aanchal Gupta, Microsoft, 21 January 2022.

64. “The Winter Getaway That Turned the Software World Upside Down,” by Caroline Mimbs Nyce, The Atlantic, 8 December 2017.

65. “The Story behind the Microsoft Security Development Lifecycle,”by Rod Trent, ITPro Today, 7 March 2014.

66. “The History of Penetration Testing,” Infosec Resources, 4 September 2021.

67. “The Passing of a Pioneer,” CERIAS Blog, Purdue, 2013.

68. "Computer Security Threat Monitoring and Surveillance," by James Anderson, csrc.nist.gov, 26 February 1980.

69. “Kriegsspiel – How a 19th Century Table-Top War Game Changed History,” by MilitaryHistoryNow.com, 19 April 2019.

70. “Computer Fraud and Abuse Act (CFAA),” NACDL - National Association of Criminal Defense Lawyers, 2022.

71. “Electronic Communications Privacy Act (ECPA),” by EPIC (Electronic Privacy Information Center), 2016.

72. “2600: The Hacker Quarterly,” by Encyclopædia Britannica, 2022.

73. “Early Hackers Used Whistles from Cap’n Crunch Cereal Boxes,” by Anne Ewbank, Atlas Obscura, 18 May 2018.

74. "Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers," by Andy Greenberg, Published by Doubleday, 7 May 2019.

75 “How the IBM PC Won, Then Lost, the Personal Computer Market,” by James Cortada, IEEE Spectrum, 21 July 2021.

76. "Tubes: A Journey to the Center of the Internet,” by Andrew Blum, Published by Ecco, 1 January 2012.

77. “A Short History of the Internet,” by the National Science and Media Museum, 2020.

78. “The Lost Civilization of Dial-Up Bulletin Board Systems,” by Benj Edwards, The Atlantic, 4 November 2016.

79. “The Birth of GDPR: What Is It and What You Need to Know,” by Andrew Rossow, Forbes, 10 December, 2021.

80. “Collapse of the Soviet Union | Causes, Facts, Events, & Effects,” by Encyclopædia Britannica, 2022.

81. “Security and Privacy Laws, Regulations, and Compliance: The Complete Guide.” CSO staff. 2021, 3 September 2021.

82. “Program Basics,” by FedRAMP.gov, 2022.

83. “Security and Privacy Laws, Regulations, and Compliance: The Complete Guide,” CSO staff, CSO Online, 3 September 2021.

84. “Security and Privacy Laws, Regulations, and Compliance: The Complete Guide.” CSO Staff, CSO Online, 3 September 2021.

85. “Security and Privacy Laws, Regulations, and Compliance: The Complete Guide,” CSO Staff, CSO Online, 3 September 3 2021.

86. “Security and Privacy Laws, Regulations, and Compliance: The Complete Guide,” CSO Staff, CSO Online, 3 September 3 2021.

87. “History and Creation of the Framework,” by Nicole Keller, NIST, 8 February 2018.

88. “The History of Computing: DEF CON: A Brief History of the Worlds Largest Gathering of Hackers,” by Charles Edge, Thehistoryofcomputing.net, 2022

89. “25 Years Later: Looking Back at the First Great (Cyber) Bank Heist,” by Zia Hayat, Dark Reading, 2 January 2019.

90. “CISO Conversations: Steve Katz, the World’s First CISO,” by Kevin Townsend, Securityweek.com, 1 December 2021.

91. “The Start of OWASP – a True Story,” by Mark Curphey, Veracode, 26 May 2014.

92. “About the Building Security in Maturity Model,” BSIMM.” Bsimm, 2021.

93. “The Phoenix Project: A Novel About IT, DevOps, and Helping Your Business Win,” by Gene Kim, Kevin Behr, and George Spafford, Published by IT Revolution Press, 10 January 2013.

94. “Cult of the Dead Cow: How the Original Hacking Supergroup Might Just Save the World,”by Joseph Menn, Published by PublicAffairs, 4 June 2019.

95. “Recognizing and Adapting To Unrestricted Warfare Practices by China,” by COL Bryan K. Luke, Air War College, 15 February 2012

96. “Unrestricted Warfare : China’s Master Plan to Destroy America,” by Qiao Liang and Wang Xiangsui, Published by Pan American Publishing Company, February 1999.

97. "Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," by Bryan Krekel, George Bakos, Christopher Barnett, Northrop Grumman Corporation Information Systems Sector, The US-China Economic and Security Review Commission, October 2009.

98. “The Full Story of the Stunning RSA Hack Can Finally Be Told,” by Andy Greenberg, Wired, 20 May 2021.

99. "The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation," by Committee on Oversight and Government Reform US House of Representatives, 114th Congress, 7 September 2016.

100. “A Bunch of Hacks,” by CSO Staff, CSO Online, April 2004.

101. “U.S. Cyber Command,” by Command History, Cybercom.mil, 2020.

102. “An Approach For Using Probabilistic Risk Assessment In Risk-Informed Decisions On Plant-Specific Changes To The Licensing Basis: Regulatory Guide 1.174, Revision 3,” by Anders Gilbertson, US Nuclear Regulatory Commission, January 2018.

103. “Firewalls and Internet Security: Repelling the Wily Hacker,” by William Cheswick and Steven Bellovin, Published by Addison-Wesley Professional, 28 April 1994.

104. Dr. Fred Cohen, Rick Howard, Phone Conversation, 29 August 2016.