THE HISTORY OF CYBERTHREATS

History is a good teacher. Knowing the history of cyberthreats provides a better understanding of how we got here—and helps us prepare the resources we’ll need to battle them in the future better.

PRE-CYBER ERA
THE RISE OF THE WORM
- 1940s: The possibility of replicating computer programs is floated.
- 1950s: Core Wars, a game that uses for control of the computer, launches.
- 1960s: Game of life, a life-emulating program, comes to life.
- 1971: “I’m the creeper, catch me if you can” scrolls across computer screens.

THE CONTAGION ERA
THE RISE OF VIRAL ATTACKS
- 1983: Patent for a “cryptographic communications system and method” is granted.
- 1983: The term “computer virus” is born.
- 1986: The “Pakistani Brain” virus becomes the first to cause serious damage.
- 1986: The U.S. passes the Computer Fraud and Abuse Act (CFAA).
- 1988: Robert T. Morris releases the Morris Worm and is convicted under CFAA.

THE LONE WOLF ERA
THE RISE OF ME-TOO ATTACKS
- 1993: DEF CON Conference launches with 100 attendees.
- 1995: Secure Sockets Layer (SSL) becomes online purchasing standard.
- 2000: Mafiaboy brings down major websites, causing an estimated $7.5 million in damages.
- 2000: ILOVEYOU virus attacks tens of millions of Windows PCs, causing email systems to crash.

THE CROWDSOURCING ERA
THE RISE OF TARGETED ATTACKS
- 2006: More than 45.7 million customer records stolen in T.J. Maxx Company attack.

THE CYBERWAR ERA
THE RISE OF NATION-STATE ATTACKS
- 2010: Google announces an attack on its infrastructure in China.
- 2017: Linked to Russian intelligence, APT28 (Fancy Bear), launches a cyberespionage campaign against the Montenegrin government.
- 2018: China breaches the computers of U.S. government agencies and major corporations, ending a 13-year cyberespionage campaign that was later found to affect as many as 12 other countries.

THE CROWDSOURCING ERA
THE RISE OF TARGETED ATTACKS
- 2006: More than 45.7 million customer records stolen in T.J. Maxx Company attack.

THE CONTAGION ERA
THE RISE OF VIRAL ATTACKS
- 1983: Patent for a “cryptographic communications system and method” is granted.
- 1983: The term “computer virus” is born.
- 1986: The “Pakistani Brain” virus becomes the first to cause serious damage.
- 1986: The U.S. passes the Computer Fraud and Abuse Act (CFAA).
- 1988: Robert T. Morris releases the Morris Worm and is convicted under CFAA.

THE LONE WOLF ERA
THE RISE OF ME-TOO ATTACKS
- 1993: DEF CON Conference launches with 100 attendees.
- 1995: Secure Sockets Layer (SSL) becomes online purchasing standard.
- 2000: Mafiaboy brings down major websites, causing an estimated $7.5 million in damages.
- 2000: ILOVEYOU virus attacks tens of millions of Windows PCs, causing email systems to crash.

THE CROWDSOURCING ERA
THE RISE OF TARGETED ATTACKS
- 2006: More than 45.7 million customer records stolen in T.J. Maxx Company attack.

THE CYBERWAR ERA
THE RISE OF NATION-STATE ATTACKS
- 2010: Google announces an attack on its infrastructure in China.
- 2017: Linked to Russian intelligence, APT28 (Fancy Bear), launches a cyberespionage campaign against the Montenegrin government.
- 2018: China breaches the computers of U.S. government agencies and major corporations, ending a 13-year cyberespionage campaign that was later found to affect as many as 12 other countries.

THE FUTURE
THE RISE OF THE CYBERSECURITY LAB SHORTAGE
- Even as cyberthreats become more routine, they’re becoming more sophisticated.
- Yet the biggest threat may be the lack of skilled professionals to deal with the onslaught of attacks.

AS ONE EXPERT SAYS:
“The greatest virtual threat today is not state-sponsored cyber-attacks; newfangled clandestine malware, or a hacker culture run amok. The most dangerous looming crisis in information security is instead a severe cybersecurity labor shortage...”

WHICH BEGS THE QUESTION:
HOW CAN THE CYBERWAR BE WON WITH FEW RESOURCES ON THE BATTLEFIELD?

INTRODUCING THE TECH DATA CYBER RANGE.
This real-world, hands-on learning center helps IT and cybersecurity professionals learn how to respond to the latest threats in a live environment.

It’s just one way we help prepare you for the cybersecurity world to come.