security

noun  se·cu·ri·ty  \si-ˈkyu-ər-ə-tē\  
the quality or state of being secure: such as  

a : freedom from danger : safety  
b : freedom from fear or anxiety  
c : freedom from the prospect of being laid off
  "job security"
What is computer security?

Keeping systems, programs, and data "safe"

The CIA Triad*:

1. Confidentiality
2. Integrity
3. Availability

*No relationship to the Central Intelligence Agency
Confidentiality

• Keep data & resources hidden
  – Data will only be shared with authorized individuals
  – Sometimes – conceal the existence of data or communication

• Traditional focus of computer security
  – Usually accomplished with access control and encryption

Data confidentiality:

“The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [i.e., to any unauthorized system entity].”

– RFC 4949, Internet Security Glossary
Confidentiality vs. privacy

Privacy
- Limit what information can be shared with others
- Ability to send messages anonymously
- Control other’s use of information about you
- Freedom from intrusion

The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share its personal information with others.

See: HIPAA, personal information, Privacy Act of 1974, RFC 4949, Internet Security Glossary

Privacy is a reason for confidentiality

Secrecy: hiding the existence of information; the ability to conceal messages or exchange messages without anyone else seeing them
Privacy is increasingly harder to attain

• “Free services”
  – Facebook, Google, Twitter, LinkedIn, Instagram, TikTok, …
  – Information collection, browser cookies to track web access

• More data is online and widely accessible
  – No need to go to town hall to get real estate transactions

• Phone companies know every place you go

• Big data analytics
  – It’s increasingly easy to correlate data:
    Credit card spending, travel, jobs, marriages/divorces, kids, cars, …

• This can be good and bad
EXIF data in photos captures the time & place of the photo – creating a chronological log of your travels
Privacy & data mining … on a national level

• U.S. credit scores
  – Credit reporting companies track employment, spending, home ownership, loan repayment, …
  – Credit scores affect ability to borrow money, buy a home

• China’s social credit system
  – Track trustworthiness of everyday citizens, corporations, and government officials
  – Track behavior
    • Frivolous spending, major & minor infractions (smoking in a no-smoking zone)
  – Boost public confidence and fight problems like corruption and business fraud
Integrity

- The trustworthiness of the data or resources
- Preventing unauthorized changes to the data or resources

**Data integrity**
- Property that data has not been modified or destroyed in an unauthorized or accidental manner

**Origin integrity**
- Authentication

**System integrity**
- The ability of a system to perform its intended function, free from deliberate or inadvertent manipulation

**Often more important than confidentiality!**
Availability

- Being able to use the data or resources
- Property of a system being accessible and capable of working to required performance specifications

Turning off a computer provides confidentiality & integrity but hurts availability

*Denial of Service (DoS) attacks target availability*
Citi Bike riders were left stranded on Wednesday after an outage at an Amazon data center knocked out service to the bike-share system during the height of the morning rush hour.

The disruption began shortly after 7:00 a.m., sparking complaints and confusion from monthly subscribers unable to unlock a bike. A spokesperson for Lyft, the Citi Bike parent company, said stations were beginning to come back online as of 9:20 a.m., though some riders continued to report issues.

Outside Bellevue Hospital in Manhattan on Wednesday morning, would-be commuters stood in front of a docking station fruitlessly trying to connect to the bikes with their phones.
University loses 77TB of research data due to backup error

Bill Toulas • December 30, 2021

The Kyoto University in Japan has lost about 77TB of research data due to an error in the backup system of its Hewlett-Packard supercomputer.

The incident occurred between December 14 and 16, 2021, and resulted in 34 million files from 14 research groups being wiped from the system and the backup file.

After investigating to determine the impact of the loss, the university concluded that the work of four of the affected groups could no longer be restored. All affected users have been individually notified of the incident via email, but no details were published on the type of work that was lost.

At the moment, the backup process has been stopped. To prevent data loss from happening again, the university has scrapped the backup system and plans to apply improvements and re-introduce it in January 2022.
Terabytes of Deleted Case Data Forces Dallas PD to Revise Policy

A Dallas Police employee accidentally deleted 22 TBs of case files when trying to migrate data between servers. Officials say they’re now working to recover what they can and prevent future issues.

Jule Pattison-Gordon • August 17, 2021

In Dallas, at least one murder trial has been delayed after a police employee accidentally destroyed 8 terabytes of digital case files and materials during a routine data migration process gone wrong.

A Dallas Police Department (DPD) employee attempting to move older case files out of a cloud-based archive and onto an on-premise server housed in the city’s data center accidentally deleted 22 terabytes worth of files, the DPD told media in an emailed statement.

Police recovered 14 terabytes, but DPD believes the remaining 8 terabytes are “permanently deleted and unrecoverable from the archive location,” per its statement.

The impacted files include audio recordings, case notes, images, videos and other materials, the DPD said. According to an Aug. 11 memo released by the Dallas County Criminal District Attorney’s Office, the data loss affects prosecution of cases for which the offending event occurred before July 28, 2020.
Thinking about security

**Security is not**
- adding encryption
- … or using a 512-bit key instead of a 64-bit key
- … or changing passwords
- … or setting up a firewall

**It is a systems issue**
= Hardware + firmware + OS + app software + networking + people
= Processes & procedures, policies, detection, forensics

“Security is a chain: it’s only as secure as the weakest link”
– Bruce Schneier
Security is hard

• **Software is complex**
  - Windows 10: ~50 million lines of code
  - Google services comprise ~2 billion lines of code
  - Linux distribution: over 200 million lines of code
    - Linux kernel: 27.8M lines of code across 66,492 files
    - Linux kernel in 2021: 73,700 commits from 4,421 different authors
    - 3.2 million lines of new code added and 1.3 million lines removed

  
  
  
  Try to find the bugs!

• **Systems are complex**
  - Lots of layers: microcode + firmware + OS + libraries + apps + devices
  - Lots of elements: clients, servers, networks, embedded devices
  - Interaction with cloud services
  - Third party components
  - Complex interaction models
  - All parts are not always under control of one administrator

• **Human factor**
  - People make mistakes
Some big data breaches

Exfiltration
Some big data breaches

- **CAM4** – March 2020
  - 10.88 billion user accounts; 11 million email addresses
  - Full names, chat transcripts, payment logs

- **SolarWinds** – December 2020
  - Supply chain attack
  - 18,000 companies compromised

- **Yahoo** – October 2017
  - Three billion user accounts compromised
  - Names, security questions & answers

- **Aadhaar** – March 2018
  - Personal information of more than one billion Indian citizens stored in the world’s largest biometric database
  - Names, unique identity numbers, bank details, photos, thumbprints, retina scans
Some big data breaches

• **First American Financial Corp.** – May 2019
  – 885 million user’s records leaked dating back more than 16 years
  – Bank accounts, social security numbers, wire transaction, mortgages

• **Verifications.io** – February 2019
  – Email validation service exposed 763 million unique addresses
  – Public MongoDB instance with no password
  – Names, phone numbers, dates of birth, genders

• **LinkedIn** – June 2021
  – Information on 700 million (92% of all users) users posted for sale on the Dark Web
  – Obtained by using LinkedIn’s API
  – Email addresses, names, phone numbers, experience
Some big data breaches

• Facebook – April 2019
  – Two 3rd-party app datasets exposed to public Internet
  – Contains comments, likes, reactions, account names
  – 540 million users affected

• Marriott – November 2018
  – Data from about 500 million Starwood hotel customers from 2014-2016
  – Names, contact info, passport numbers, Preferred Guest numbers, etc.
  – Credit & debit card numbers and expiration dates from 100 million customers

• Adult Friend Finder – October 2016
  – 20 years of data from six databases
  – Names, email addresses, passwords
COMB: largest breach of all time leaked online with 3.2 billion records

Bernard Meyer • February 12, 2021

It’s being called the biggest breach of all time and the mother of all breaches: COMB, or the Compilation of Many Breaches, contains more than 3.2 billion unique pairs of cleartext emails and passwords. While many data breaches and leaks have plagued the internet in the past, this one is exceptional in the sheer size of it. To wit, the entire population of the planet is at roughly 7.8 billion, and this is about 40% of that.

However, when considering that only about 4.7 billion people are online, COMB would include the data of nearly 70% of global internet users (if each record was a unique person). For that reason, users are recommended to immediately check if their data was included in the leak. You can head over to the CyberNews personal data leak checker now.

…

So how did the COMB data leak happen?

On Tuesday, February 2, COMB was leaked on a popular hacking forum. It contains billions of user credentials from past leaks from Netflix, LinkedIn, Exploit.in, Bitcoin and more. This leak is comparable to the Breach Compilation of 2017, in which 1.4 billion credentials were leaked.

However, the current breach, known as “Compilation of Many Breaches” (COMB), contains more than double the unique email and password pairs. The data is currently archived and put in an encrypted, password-protected container.

Ransomware attacks

- Colonial Pipeline – May 2021 — Stopped fuel delivery – $4.4M
- JBS Meats – May 2021 – Stopped meat delivery – $11M
- Acer – March 2021 – demanded $50M
- Brenntag – chemical distribution – $4.4M
- Kaseya – IT monitoring – 800-1500 businesses – demanded $70M
- Quanta – contract manufacturing (Apple) – demanded $50M
- AXA – insurance – $??
Large-scale ransomware: 2016 – Petya

Encrypting malware that targets Microsoft Windows systems
- Ransom ~$400 & doubles after each week
- Infected millions of computers

June 2017 – NotPetya – new variant of Petya launched
- Spread via software update mechanism of a Ukrainian tax preparation program
- Disguised as ransomware
- Damages estimated to be over $10 billion
- Russian government blamed
  - Used EternalBlue exploit, believed to have been developed by the U.S. NSA
Just a few recent security attacks
Log4J: software supply chain vulnerability

FTC warns companies to remediate Log4j security vulnerability

By: This blog is a collaboration between CTO and DPIP staff and the AI Strategy team | Jan 4, 2022 9:19AM

Log4j is a ubiquitous piece of software used to record activities in a wide range of systems found in consumer-facing products and services. Recently, a serious vulnerability in the popular Java logging package, Log4j (CVE-2021-44228) was disclosed, posing a severe risk to millions of consumer products to enterprise software and web applications. This vulnerability is being widely exploited by a growing set of attackers.

When vulnerabilities are discovered and exploited, it risks a loss or breach of personal information, financial loss, and other irreversible harms. The duty to take reasonable steps to mitigate known software vulnerabilities...
Hackers hijacked the popular **UA-Parser-JS** NPM library, with millions of downloads a week, to infect Linux and Windows devices with cryptominers and password-stealing trojans in a supply-chain attack.

The **UA-Parser-JS** library is used to parse a browser’s user agent to identify a visitor’s browser, engine, OS, CPU, and Device type/model.

The library is immensely popular, with millions of downloads a week and over 24 million downloads this month so far. In addition, the library is used in over a thousand other projects, including those by Facebook, Microsoft, Amazon, Instagram, Google, Slack, Mozilla, Discord, Elastic, Intuit, Reddit, and many more well-known companies.

On October 22nd, a threat actor published malicious versions of the UA-Parser-JS NPM library to install cryptominers and password-stealing trojans on Linux and Windows devices.

According to the developer, his NPM account was hijacked and used to deploy the three malicious versions of the library.
That Cream Cheese Shortage You Heard About? Cyberattacks Played a Part

Elizabeth Elkin and Deena Shanker • December 9, 2021

The cream cheese shortage wreaking havoc on bagel shops and bakeries is, in part, due to a cyberattack on the biggest U.S. cheese manufacturer.

Schreiber Foods in Wisconsin, which makes cheese slices for most of the top burger chains in America and has a cream cheese business rivaling Kraft’s, closed for days in October after hackers compromised its plants and distribution centers. While that may not sound like a long time, the company is big enough that the lost production shook U.S. markets.

Making the situation worse, the shutdown occurred at the height of cream cheese demand. Americans are doing more holiday baking and buying more cakes, and cream cheese is a common dessert ingredient. …

Cyberattacks have added to the chaos afflicting global food supply chains in the Covid-19 era, with inflation driving prices to around decade highs. Hackers also targeted meat giant JBS SA and an Iowa grain cooperative this year.

The Candy Corn Has Been Hacked

As everybody readies for spooky season, hackers have done gone and messed with a holiday staple.

Lucas Ropek • October 22, 2021

Just in time for Halloween, a ransomware gang has targeted Ferrara Candy—the massive confectionary responsible for producing Brach’s well-known candy corn—the most OG of holiday treats.

Ferrara, which is based in Chicago, is responsible for 85 percent of the candy corn production in the country during the Halloween season—and reportedly churns out approximately seven billion pieces of the candy per year.

When reached for comment, Ferrara confirmed to Gizmodo that an attack had occurred on Oct. 9 that “encrypted some of our systems.” The company further stated that it was working together with law enforcement to investigate the incident:

... The company further stated that it had resumed production in certain facilities and that it was “near to capacity” when it came to shipping from all of its distribution centers across the country. “We want to assure consumers that Ferrara’s Halloween products are on shelves at retailers across the country ahead of the holiday,” the company said.

https://gizmodo.com/the-candy-corn-has-been-hacked-1847901307
One cybersecurity expert says the cyberattack on the Newfoundland and Labrador health-care system may be the worst in Canadian history, and has implications for national security.

David Shipley, the CEO of a cybersecurity firm in Fredericton, said he's seen similar breaches before, but usually on a smaller scale.

"We've never seen a health-network takedown this large, ever," Shipley said in an interview with CBC News. "The severity of this is what really sets it apart."

Discovered on Saturday morning, the cyberattack has delayed thousands of appointments and procedures this week, including almost all non-emergency appointments in the Eastern Health region.

After refusing to confirm the cause of the disruption for days, Health Minister John Haggie said Wednesday the system has been victim of a cyberattack.

Ransomware encrypts South Africa's entire Dept of Justice network

Subtitle

Ionut Ilascu • September 15, 2021

The justice ministry of the South African government is working on restoring its operations after a recent ransomware attack encrypted all its systems, making all electronic services unavailable both internally and to the public.

As a consequence of the attack, the Department of Justice and Constitutional Development said that child maintenance payments are now on hold until systems are back online.

All services affected
The incident happened on September 6 and the department activated the contingency plan for such events to ensure the continuation of some activity in the country.

“[The attack] has led to all information systems being encrypted and unavailable to both internal employees as well as members of the public. As a result, all electronic services provided by the department are affected, including the issuing of letters of authority, bail services, e-mail and the departmental website” - Steve Mahlangu, spokesperson for the Department of Justice and Constitutional Development

This Agency’s Computers Hold Secrets.  

Hackers Got In With One Password.

Hackers used one worker’s login information to penetrate the Law Department’s network after officials failed to implement a simple security measure.

Ashley Southall, Benjamin Weiser and Dana Rubinstein • June 18, 2021

New York City’s Law Department holds some of the city’s most closely guarded secrets: evidence of police misconduct, the identities of young children charged with serious crimes, plaintiffs’ medical records and personal data for thousands of city employees.

But all it took for a hacker to infiltrate the 1,000-lawyer agency’s network early this month was one worker’s pilfered email password, according to a city official briefed on the matter.

Officials have not said how the intruder obtained the worker’s credentials, nor have they determined the scope of the attack. But the hack was enabled by the Law Department’s failure to implement a basic safeguard, known as multifactor authentication, more than two years after the city began requiring it, according to four people with knowledge of the legal agency’s system and the incident.

The intrusion interrupted city lawyers, disrupted court proceedings and thrust some of the department’s legal affairs into disarray. And on Tuesday morning, in a conference call, Mayor Bill de Blasio admonished the heads of city agencies to shore up their cyber-defenses or face consequences in the event their agencies were hacked, according to three people who were on the call.
Twitch has confirmed that it has suffered a major data breach, and that a hacker accessed the company’s servers thanks to a misconfiguration change. “We can confirm a breach has taken place,” says a Twitch spokesperson on Twitter. “Our teams are working with urgency to understand the extent of this. We will update the community as soon as additional information is available.”

Twitch admits a hacker was able to access data that was mistakenly exposed to the internet “due to an error in a Twitch server configuration change that was subsequently accessed by a malicious third party.” The company says it has “no indication that login credentials have been exposed,” and that “full credit card numbers were not exposed.”

Hackers have so far leaked data that includes source code for the company’s streaming service, an unreleased Steam competitor from Amazon Game Studios, and details of creator payouts. An anonymous poster on the 4chan messaging board released a 125GB torrent earlier today, which they claim includes the entirety of Twitch and its commit history.
Some more things to worry about
Hacking

When a tanker vanishes, all the evidence points to Russia

In June, 37,000-tonne tanker vanished from GPS off the Russian coast. All the evidence points to Russia. But what’s really going on?

By MATT BURGESS
21 Sep 2007

or Gurvan Le Meur it started out as a regular voyage. In June this year, the captain of the 37,000-tonne Atria tanker directed his ship through the Marmara Sea, along the narrow Bosphorus Strait, and into the vast Black Sea. It was a straightforward one-and-a-half-day journey. But this changed when Le Meur...
2017 – Spear Phishing Coming From Government Servers
Fall 2018-now – Cryptojacking

Your Browser Could Be Mining Cryptocurrency For A Stranger

Cryptojacking craze that drains your CPU now done by 2,500 sites

Cryptojacking has gotten out of control

North Korean Hackers Hijack Computers to Mine Cryptocurrencies

North Korean hackers are targeting computers to mine cryptocurrencies as the regime in Pyongyang seeks to level the tech industry with traditional arms trade.
Supercomputers hacked across Europe to mine cryptocurrency

Confirmed infections have been reported in the UK, Germany, and Switzerland. Another suspected infection was reported in Spain.

Catalin Cimpanu • May 16, 2020

Multiple supercomputers across Europe have been infected this week with cryptocurrency mining malware and have shut down to investigate the intrusions.

Security incidents have been reported in the UK, Germany, and Switzerland, while a similar intrusion is rumored to have also happened at a high-performance computing center located in Spain.

The first report of an attack came to light on Monday from the University of Edinburgh, which runs the ARCHER supercomputer. The organization reported "security exploitation on the ARCHER login nodes," shut down the ARCHER system to investigate, and reset SSH passwords to prevent further intrusions.
Potential for bodily harm

US warns of unusual cybersecurity flaw in heart devices

The Homeland Security Department warned Tuesday about an unusual cybersecurity flaw for one manufacturer's implantable heart devices that it said could allow hackers to remotely take control of a person's defibrillator or pacemaker.

Jan. 10, 2017, at 7:07 p.m.

By TAMI ABDOLLAH and MATTHEW PERRONE, Associated Press

WASHINGTON (AP) — The Homeland Security Department warned Tuesday about an unusual cybersecurity flaw for one manufacturer's implantable heart devices that it said could allow hackers to remotely take control of a person's defibrillator or pacemaker.

Information on the security flaw, identified by researchers at MedSec Holdings in reports months ago, was only formally made public after the manufacturer, St. Jude Medical, made a software repair available Monday. MedSec is a cybersecurity research company that focuses on the health-care industry.

The government advisory said security patches will be rolled out automatically over months to patients with a device transmitter at home, as long as it is plugged in and connected to the company's network. The transmitters send heart device data back to medical professionals.

Abbott Laboratories' St. Jude said in a statement it was not aware of deaths or injuries
The Big Tesla Hack: A hacker gained control over the entire fleet, but fortunately he’s a good guy

Fred Lambert • August 27, 2020

A few years ago, a hacker managed to exploit vulnerabilities in Tesla’s servers to gain access and control over the automaker’s entire fleet.

In July 2017, Tesla CEO Elon Musk got on stage at the National Governors Association in Rhode Island and confirmed that a “fleet-wide hack” is one of Tesla’s biggest concerns as the automaker moves to autonomous vehicles.

He even presented a strange scenario that could happen in an autonomous future:

“\textit{In principle, if someone was able to say hack all the autonomous Teslas, they could say – I mean just as a prank – they could say ‘send them all to Rhode Island’ [laugh] – across the United States… and that would be the end of Tesla and there would be a lot of angry people in Rhode Island.}”

What Musk knew that the public didn’t was that Tesla got a taste of that actually happening just a few months prior to his talk.

https://electrek.co/2020/08/27/tesla-hack-control-over-entire-fleet/
Cops Hijack Botnet, Remotely Wipe Malware From 850,000 Computers

Police in France took down a large cryptocurrency-mining malware operation with the help of a cybersecurity firm.

By Lorenzo Franceschi-Bicchierai • Aug 28 2019, 4:10pm

French police, with help from an antivirus firm, took control of a server that was used by cybercriminals to spread a worm programmed to mine cryptocurrency from more than 850,000 computers. Once in control of the server, the police remotely removed the malware from those computers.
A ransomware gang shut down after Cybercom hijacked its site and it discovered it had been hacked

Ellen Nakashima, Dalton Bennett • November 3, 2021

A major overseas ransomware group shut down last month after a pair of operations by U.S. Cyber Command and a foreign government targeting the criminals’ servers left its leaders too frightened of identification and arrest to stay in business, according to several U.S. officials familiar with the matter.

The foreign government hacked the servers of REvil this summer, but the Russian-speaking criminal group did not discover it was compromised until Cybercom last month blocked its website by hijacking its traffic, said the officials who spoke on the condition of anonymity because of the matter’s sensitivity.

Cybercom’s action was not a hack or takedown, but it deprived the criminals of the platform they used to extort their victims — businesses, schools and others whose computers they’d locked up with data-encrypting malware and from whom they demanded expensive ransoms to unlock the machines, the officials said.

In the hours after the Cybercom operation, which has not been previously reported, one of REvil’s leaders saw the site’s traffic had been redirected.

“Domains hijacked from REvil,” wrote 0_neday, an REvil leader, on a Russian-language forum popular with cyber criminals, on Oct. 17.
For six months, security researchers have secretly distributed an Emotet vaccine across the world

Binary Defense researchers have identified a bug in the Emotet malware and have been using it to prevent the malware from making new victim

Catalin Cimpanu • August 14, 2020

Most of the time, fighting malware is a losing game. Malware authors create their code, distribute payloads to victims via various methods, and by the time security firms catch up, attackers make small changes in their code to quickly regain their advantage in secrecy. …

However, not all malware operations can be hurt this way. Some cyber-criminals either reside in countries that don’t extradite their citizens or have a solid knowledge of what they’re doing.

Emotet is one of the gangs that check both boxes. Believed to operate from the territories of the former Soviet States, Emotet is also one of today’s most skilled malware groups, having perfected the infect-and-rent-access scheme like no other group.

The malware, which was first seen in 2014, evolved from an unimportant banking trojan into a malware swiss-army knife that, once it infects victims, it spreads laterally across their entire network, pilfers any sensitive data, and turns around and rents access to the infected hosts to other groups.

https://www.zdnet.com/article/for-six-months-security-researchers-have-secretly-distributed-an-emotet-vaccine-across-the-world/
US military has reportedly acted against ransomware groups

Action came after a series of crippling attacks raised concerns about vulnerabilities in the nation's critical infrastructure.

Steven Musil • December 5, 2021

The US military has gone on the offensive against ransomware groups as US companies increasingly become targets of malware attacks, the nation’s top cyber defender acknowledged on Saturday.

Up until about nine months ago, reining in ransomware attacks was seen as the responsibility of law enforcement agencies, Gen. Paul M. Nakasone, the head of US Cyber Command and director of the National Security Agency, told the New York Times. But attacks like the ones on Colonial Pipeline and JBS beef plants have been "impacting our critical infrastructure," Nakasone said, leading federal agencies to ramp up the gathering and sharing of intelligence on ransomware groups.

"The first thing we have to do is to understand the adversary and their insights better than we've ever understood them before," Nakasone said in an interview at the Reagan National Defense Forum, a gathering of national security officials.

Nakasone didn't describe the action taken or identify the groups targeted, but said one of the goals is to "impose costs" for ransomware groups.

https://www.cnet.com/tech/services-and-software/us-military-has-reportedly-acted-against-ransomware-groups/
The End