تکامل از امنیت اطلاعات به تاب‌آوری سایبری

Unpacking Cyber Resilience

Whitepaper

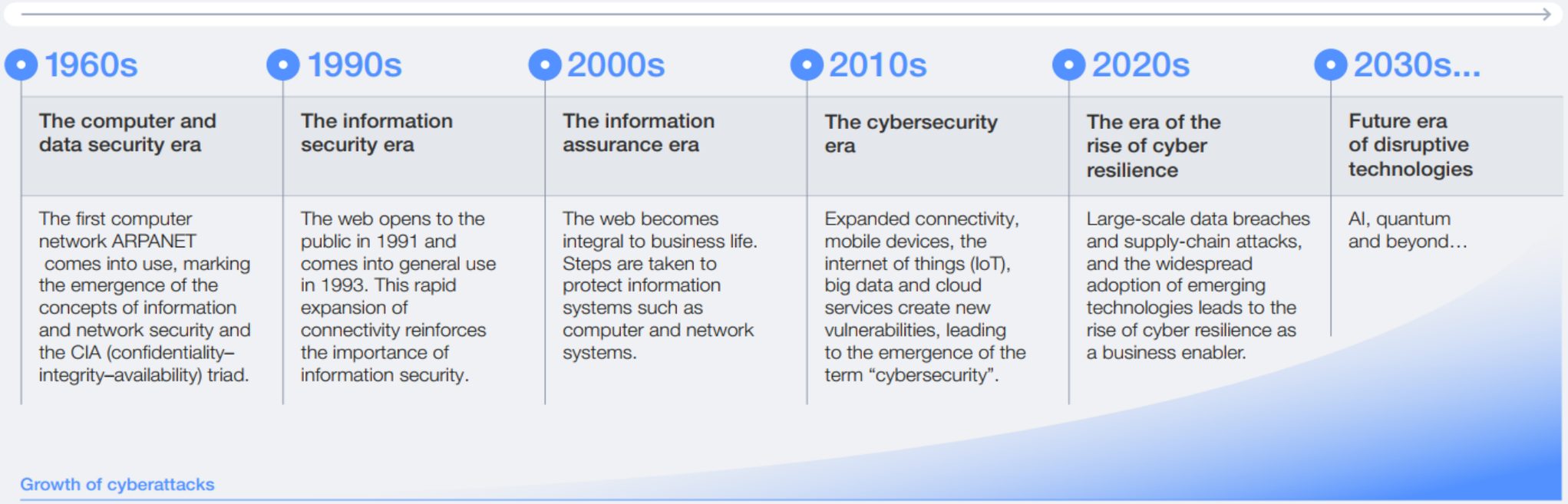
NOVEMBER 2024

WEF in Collaboration with the University of Oxford

صیامی

Page Size: A3

FIGURE 1 | **The evolution from information security to cyber resilience**



Theft by computer (1960), early evidence of criminals exploring vulnerabilities to steal and compromise data from shared resources.

The Creeper virus (1971), the first computer virus, affected all 28 machines running the TENEX operating system.

The Morris worm (1988) caused widespread damage, deleting the resources of 6,000 machines.

The Melissa virus (1999) overloaded the email servers of more than 300 businesses and government agencies, causing $80 million in damage.

The ILOVEYOU virus (2000) caused significant disruption and $15 billion in damage worldwide.

The US Department of Defense (DoD) and NASA hack (2000) placed NASA systems offline for 21 days.

The Slammer worm (2003) caused a denial of service affecting internet hosts and slowing the internet, while infecting more than 75,000 victims in less than 10 minutes.

The Estonia cyberattack (2007) where a series of targeted attacks took down Estonian banks, media outlets and government bodies.

Stuxnet (2010) was the first attack targeting industrial control systems (ICS) to have physical consequences.

The Sony PlayStation hack (2011) stole 77 million account holders' personal information.

Shammon malware (2012) affected several IT machines, disrupting industrial operations for more than two weeks.

BlackEnergy (2015) targeted Ukraine's power grid, causing significant power outages.

Triton (2017) was a malicious code that disabled safety systems to prevent industrial and physical accidents, costing $1 trillion.

NotPetya ransomware (2017) cost multiple large organizations more than $10 billion.

WannaCry ransomware (2017) infected more than 230,000 computers, causing billions of dollars of damage.

The Equifax data breach (2017) affected 143 million customers and cost $1.4 billion in recovery.

Solarwinds (2020) supplied malicious code to 18,000 customers, with 11% of revenue lost.

The Irish Health Service Executive attack (2021) caused disruption for several months, with a total response cost exceeding €100 million.

Colonial Pipeline ransomware (2021) crippled fuel supplies to 50 million Americans for 11 days, costing $4.4 million and brand damage.

Log4J (2021) peaked at 100 attacks every minute, affecting more than 40% of all business networks globally.

The Okta data breach (2022) affected 366 customers in just five days (16–21 January), leading to a $2 billion market cap loss.

The MOVEit transfer data breach (2023) affected 94 million users, more than 2,500 businesses and caused more than $10 billion in damage.

Note: Illustrative view, not exhaustive.

Source: Analysis by the World Economic Forum and the University of Oxford

تکامل از امنیت اطلاعات به تاب‌آوری سایبری

2030s

دوره آینده و فناوری‌های خلاقانه

هوش مصنوعی، پردازش کوانتومی و فراتر از آن

2020s

دوره خیزش تاب‌آوری سایبری

نشت داده‌های کلان‌مقیاس، حملات زنجیره تامین و گسترده شدن سازگاری با فناوریهای نوظهور منجر بدان شد که تاب‌آوری سایبری به‌عنوان یک پشیران کسب‌وکار مطرح شود

سولارویندز (۲۰۲۰): ارائه کد مخرب به ۱۸ هزار مشتری و از دست رفتن ٪۱۱ درآمد

حمله به خدمات درمانی ایرلند (۲۰۲۱): ماه‌ها اختلال، هزینه رفع ۱۰۰ میلیون یورو

باج‌افزار کلونیال پایپ‌لاین (۲۰۲۱): ایجاد اختلال ۱۱ روزه در تامین سوخت آمریکا با ۴/۴ میلیون دلار هزینه

لاگ‌فورجی (۲۰۲۱): در اوج خود به ۱۰۰ حمله در دقیقه رسید و ٪۴۰ از کل شبکه‌های تجاری در جهان را تحت تأثیر قرار داد.

نشت داده‌های اکتا (۲۰۲۲):در پنج روز ۳۶۶ مشتری را تحت تأثیر، از دست رفتن ۲ میلیارد دلار ارزش بازا.

نشت داده‌های موو ایت ترنسفر (۲۰۲۳): ۹۴ میلیون کاربر و بیش از ۲۵۰۰ کسب‌وکار را تحت تأثیر، بیش از ۱۰ میلیارد دلار خسارت

2010s

دوره امنیت سایبری

توسعه دسترس‌پذیری، ابزارهای موبایلی، اینترنت اشیاء، کلان داده، خدمات ابری آسیب‌پذیریهای جدیدی را به وجود آورده و باعث ظهور واژه امنیت سایبری شد.

استاکس‌نت (۲۰۱۰): نخستین حمله به سامانه‌های کنترل صنعتی

هک پلی‌استیشن سونی (۲۰۱۱): سرقت ۷۷ میلیون اطلاعات شخصی کاربران

بدافزار شامون (۲۰۱۲): ایجاد وقفه در عملیات صنعتی برای بیش از دو هفته

انرژی سیاه (۲۰۱۵): باعث قطعی قابل برق در اوکراین

تریتون (۲۰۱۷): کد مخرب بود که سیستم‌های ایمنی جلوگیری از حوادث را غیرفعال می‌کرد، یک تریلیون دلار هزینه .

باج‌افزار نات‌پتیا (۲۰۱۷) بیش از ۱۰ میلیارد دلار به چندین سازمان بزرگ خسارت زد.

باج‌افزار و اناکرای (۲۰۱۷): بیش از ۲۳۰ هزار کامپیوتر آلوده شده، میلیاردها دلار خسارت.

نشت داده‌ها در اکویی‌فاکس (۲۰۱۷): ۱۴۳ میلیون مشتری تحت تاثیر و هزینه بازیابی ۱/۴ میلیارد دلاری

2000s

دوره اطمینان اطلاعات

بکارگیری وب درهم‌تنیده با کسب‌وکارها شد. گام‌هایی برای حفاظت از سیستم‌های اطلاعاتی همچون سیستم‌های کامپیوتری و شبکه‌ای برداشته شد.

هک وزارت دفاع و سازمان ناسا (۲۰۰۰): باعث آفلاین شدن ۲۱ روزه سامانه‌های سازمان ناسا شد.

کرم اسلامر (۲۰۰۳): باعث اختلال در سرویس‌دهی هاست‌های اینترنتی و کاهش سرعت اینترنت شد، توانست بیش از ۷۵ هزار قربانی را در کمتر از ۱۰ دقیقه آلوده کند.

حمله سایبری استونی (۲۰۰۷): مجموعه‌ای حملات هدفمند، بانک‌ها، رسانه‌ها و نهادهای دولتی استونی را از کار انداخت.

1990s

دوره امنیت اطلاعات

وب در سال ۹۱ اختراع و از سال ۹۳ جهانگیر شد. با رشد تصاعدی ارتباطات شبکه‌ای بر اهمیت امنیت اطلاعات افزوده شد.

ویروس ملیسا (۱۹۹۹): سرورهای ایمیل بیش از ۳۰۰ کسب و کار و سازمان دولتی را با بار اضافی مواجه کرد و ۸۰ میلیون دلار خسارت به بار آورد.

ویروس آی‌لاویو (۲۰۰۰): باعث اختلال قابل توجه و خسارت ۱۵ میلیارد دلاری در سراسر جهان شد.

1960s

دوره امنیت کامپیوتر و داده

نخستین شبکه کامپیوتری (آرپانت) بکار گرفته شده و باعث ظهور مفاهیم امنیت داده و شبکه شده و سه‌گانه (محرمانگی، یکپارچگی و دسترس‌پذیری) اهمیت یافت.

دزدی با کامپیوتر(۱۹۶۰): نخستین شواهد از رفتار مجرمانه که آسیب‌پذیری‌ها را بررسی و نسبت به سرقت و یا سوءاستفاده از داده‌ها از منابع مشترک اقدام می‌کردند.

ویروس کرپر(۱۹۷۱) نخستین ویروس کامپیوتری که تمام ۲۸ کامپیوتر یک شبکه را آلوده کرد.

کرم موریس(۱۹۸۸): باعث خسارت گسترده شد و منابع ۶۰۰۰ دستگاه را از بین برد.