The Growing Cybersecurity Threat: How To Take Action And Protect Yourself NOW

Presented by:

Leia Kupris Shilobod, CCP, CISM
Chief Security Officer | CEO | IT Princess of Power, CompliancyIT

www.compliancyit.io

CompliancyIT

What I Want You To Know:

- The **#1 security threat to your business** that antivirus, firewalls and other security tools can't protect against.
- Why firewalls and antivirus software **are useless** against the NEW threats happening today.
- How mobile phones and cloud applications are **seriously jeopardizing your organization's security** and data protection – and what you need to do to protect yourself.
- The strategies to **protect yourself.**

CompliancyIT

So That You're Not...

A **Sitting Duck** To Cybercriminals

Empower You To Protect Everything You've *Worked So Hard To Achieve*

CompliancyIT

Why Should You Even Care About What I Have To Say?

- **Founded** InTech/CompliancyIT as a Security focused IT Services and Cybersecurity Compliance Provider in **2006**
- Frequently **speak nation-wide** on IT Security, IT Documentation, IT Operations, CMMC | NIST 800-171, and IT for Manufacturers
- Have secured **hundreds of clients**
- Specialize in securing the Defense Industrial Base
- Certified Information Security Manager (CISM)
- Creator of the **"IT Documentation Toolkit Cybersecurity Compliance Program"**
- Co-Star and Co-Producer of move **"Cybercrime: The Dark Web Uncovered"**
- Author of:
  - **"Cyber Warfare: Protecting Your Business From Total Annihilation"**
  - **"The 3 Indisputable Rules Every Manufacturer Must Know Before Purchasing Any IT Product or Service"**

CompliancyIT

Attacks Are Becoming
More Vicious, More Frequent

- For the first time in history, **cybercrime is now the most prevalent type of crime against businesses**.
- **Identity Theft** is the most common type of consumer crime.
- All can be achieved behind a keyboard, far, far away from the victim

Internet Crime Compliant Center (IC3) Statistics - 2022

CompliancyIT

If It's So Common, Why Don't You Hear More About It?

- It's extremely embarrassing to admit you've been hacked.
- Many people ***don't even know*** they've been hacked until it's revealed in a Security Audit.
- ***Horrible PR: Do you REALLY want your clients (or patients!) to know their information was accessed?***
- The legal ramifications (fines, lawsuits, legal fees) can be *significant*, so many incidents stay hushed up.

CompliancyIT

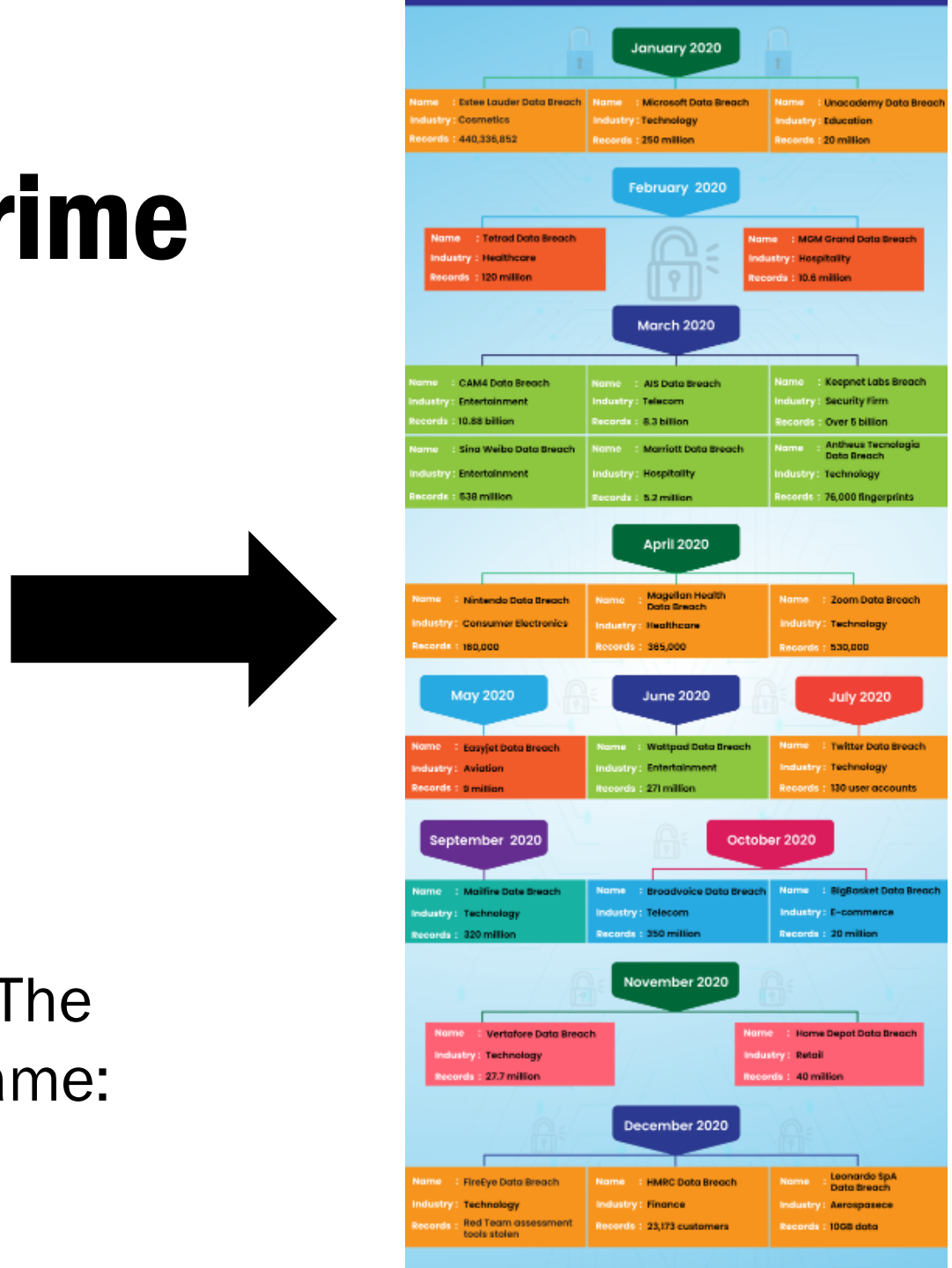
How Did We Get Here?

A Quick Overview Of The Sophistication And Proliferation Of The

Cybercrime Business

CompliancyIT

The Evolution Of Crime



The Tools Have Changed, But The Underlying Motives Are The Same:
Theft, Fraud, Blackmail

CompliancyIT

What's Motivating Them?

The Same Thing As You: Money

<u>THIS IS A BUSINESS, but without the overhead, taxes or problems most legitimate businesses face</u>.

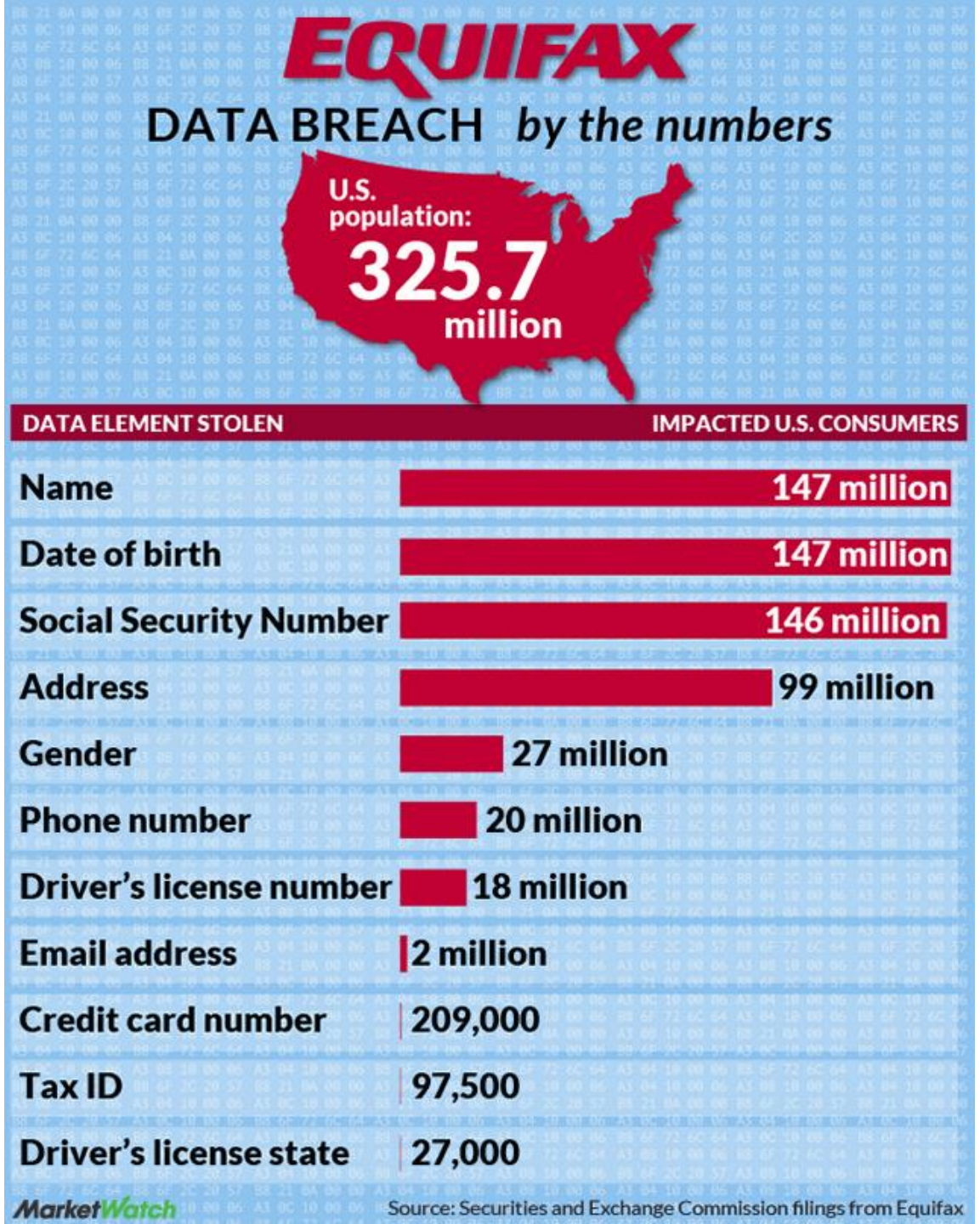
- Credit card details sell for: **$2 to $90**
- iTunes accounts sell for about: **$8**
- Physical credit cards sell for: **$190**
- **One successful ransomware hit for a business is worth $2,500 to $50,000 per incident!**
- **Even an amateur can expect to make $80,000 per month stealing and selling data.**

CompliancyIT

80 Million People HACKED

This Is A Serious BUSINESS For Hackers, Not Just A Hobby

They Are Working 365 Days A Year To Steal Data To Sell On The Dark Web And/Or Siphoning Money From Your Bank Account And Company



147 Million People HACKED

Cybercriminals Use This Data To:

- Open credit cards and take out loans in your name.
- Steal your tax refund by filing a return with your name.
- Create highly targeted phishing scams to access your bank account, e-mail, computer and network.

CompliancyIT

400+ Million People's Data Stolen, Exposed

How Cybercriminals Use This Data:

- **Blackmail**, exposing your sexual preferences and online dating history, transgressions and "interactions" unless you pay up.

What's Enabling Them?

- This is an **EASY business** to set up and run with low to no overhead.
- There are **hundreds** of websites, "exploit kits," how-to information, and services being sold to assist hackers.
- Malware **programs run on autopilot** using artificial intelligence and bots; they DO NOT require a "guy sitting at a computer" hacking *one account at a time*.
- IoT (Internet of Things) *EVERYTHING* is connected, making it easy to gain access.
- The **FBI is overwhelmed** with cases; so while your incident is BIG to you, it's "one in a million" to them (*you're on your own*).
- The **Dark Web** makes it near impossible to catch them, and there are not country borders.

What's Enabling Them?

- **Business Email Compromise** (BEC) is a leading method of attacks, with the IC3 receiving 21,832 complaints in 2023 accounting for over $2.7 BILLION in losses.
- Tech and Customer Support / Government **Impersonation** strategies defraud thousands of victims a year, accounting for over $1 BILLION in losses.
- Many of these outfits operate like LEGITIMATE BUSINESSES – **complete with comp plans, PTO, and onboarding programs.**
- **YOU. You are enabling them due to your lack of knowledge and vigilance.**

What Is The "Dark Web"?

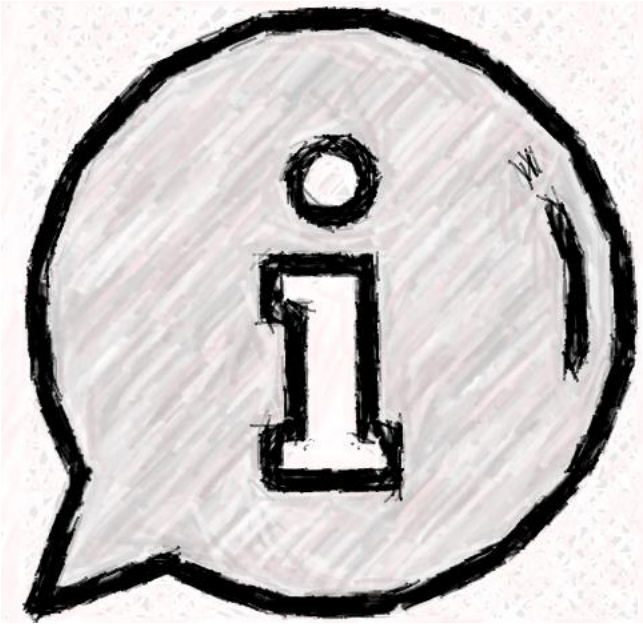
- The "**Dark Web**" is a separate, hidden part of the "World Wide Web" that is concealed from conventional search engines where cybercriminals operate.
- Cybercriminals use it because you can operate anonymously.
- It's estimated the "Dark Web" is 550 times larger than the "World Wide Web"...and growing!

Want to know more?

- Check out my documentary **“Cyber Crime: The Dark Web Uncovered”**
- Available on Amazon Movie.

But What Kind Of Information Is There?

- Credit Card Numbers
- Social Security Numbers
- PII (name, birthdate, address, phone number, etc.)
- Your health data
- Account numbers: bank, financial investments
- Usernames/email addresses and passwords
- **YOUR SENSITIVE INFORMATION**



My Information?

12/14/23	rahkeem@joepolish.com	pira*****
11/03/23	eunice@joepolish.com	rtyu*****
	joe@joepolish.com	kick*****

chrissy@joepolish.com	Emai*****
support@joepolish.com	Emai*****
polish@joepolish.com	Emai*****

gina@joepolish.com	$2a$*****
joe@joepolish.com	$2a$*****
miki@joepolish.com	$2a$*****
eunice@joepolish.com	$2a$*****

The Biggest Danger Is Your Complacency

Please **DO NOT underestimate** the importance of addressing and protecting yourself from these threats.

pliancyIT

“Only The Paranoid Survive”

“Success breeds complacency, complacency breeds failure. **Only the paranoid survive.**”

- Andrew Grove, former CEO, Intel

CompliancyIT

The #1 Threat To Your Business Is…

Your Employees!

- **Even GOOD employees make mistakes,** deleting files, clicking on phishing e-mails or innocently logging in to a compromised Facebook page.
- Employees often use **free and unsecured file-sharing applications** and cloud applications to share confidential information simply because they don't know better – and they don't think to tell you about it!
- With more people using **personal devices for work**, the "perimeter" of your network can easily be compromised, and is harder to protect.

CompliancyIT

FBI Reports More Data Breaches from Disgruntled Employees

The FBI reports seeing a spike in insider data breaches. Use these 6 strategies to fight this growing threat and prevent insider attacks on client networks.

Last week, the FBI issued a cyber security warning, stating there's been an increase in data breaches caused by disgruntled employees on or around the time they left their employer. Employees were using their access to company data to...

Disgruntled employees (and IT vendors!) who've been fired also pose a HUGE THREAT since they often have direct access to a VAST NUMBER of cloud applications and data.

CompliancyIT

Shadow IT

How Much Of Your Company's Data Is Out On Rogue Cloud Apps, Put There By Employees Who Are Just Trying To Do Their Job?

That's A GOOD Question; Do You Even Know The Answer?

BUSINESS INSIDER Tech Finance Politics Strategy Life

TECH More: Dropbox

Nearly 7 Million Dropbox Passwords Have Been Hacked

STEVE KOVACH

OCT. 13, 2014, 11:58 PM 44,024 10

FACEBOOK LINKEDIN TWITTER GOOGLE+ PRINT EMAIL

Nearly 7 million Dropbox usernames and passwords have been hacked, apparently via third-party services that hackers were able to strip the login information from.

The Next Web was the first to notice the leak on

Flickr/Ian Lamont/Dropbox In 30 Minutes

CompliancyIT

#2: Malware, Ransomware

350,000

NEW Malware Threats Are Being Released *Per Day*, And Malware Attacks Rose 79% In The Last Year

A writer once asked a literary agent, **"What kind of writing pays the most?"** Her answer was simple:

"Ransom notes."

CompliancyIT

CONSUMERAFFAIRS Consumer News Buyers Guides

Scam alert: New ransomware puts child pornography on victims' smartphones

Investigators in Tennessee uncover disturbing new twist on old ransomware scam

By Jennifer Abel

These Criminals Are Scum With

No Boundaries

CompliancyIT

Government Fines Are Escalating For Businesses

If A Device Is **Lost Or Stolen**, And The Data Was NOT Encrypted, You May Have Violated A **State Data Breach Law**

- In MOST states, "personal information" is considered a person's first name or first initial and last name in combination with a driver's license number, social security number, or any information (including logins and passwords) related to financial records (credit cards, access codes, passwords, etc.).

#3: Investment and Bank Fraud

The FDIC Does NOT Protect You From Bank Fraud, And The Bank Is NOT Responsible For Getting Your Money Back Once Stolen!!!

P.S. – It's WORSE in crypto...

Verne Harnish's Whaling of a Bad Time

8 November, 2016

For those familiar with the worlds of small business management and entrepreneurism, Verne Harnish is a venerated authority. A popular thought leader who regularly hosts panels and conferences globally, his founding credits including the **Entrepreneurs' Organization**, **Gazelles Growth Institute**, and strategic planning and executive education firm **Gazelles Inc** (a system and process used by our own company). Though a business guru by all definitions of the term, his latest newsletter illustrates that nobody can be too knowledgeable —or cautious— to be immune to **phishing** and **whaling** attacks.

Harnish recounts **a recent run-in with cyber criminals**. During a conference for leading Russian CEOs and entrepreneurs in Moscow, his email was hacked while using a public network. The assailants accessed daily updates including his organization's substantial bank balances, as well as his process with his assistant for transferring funds.

How Verne Harnish Had **$400,000** Stolen From His Bank Account

CompliancyIT

#4: Smishing and Vishing

No, its not some fancy new way to ski

- **Smishing** – fake SMS messages or DM's engineered to get you to click on links or take other actions
- **Vishing** – calls from malicious actors posing as legit services to get you to send money, access your computer, give them your credit card information
    - This just got next level with AI. Now they can sample someone's voice and an AI will generate that voice on a LIVE phone call.

CompliancyIT

Consider The Fall Out Of A Cyber Attack….

Depending On What Happens…

- **You will be BLAMED**. There's no sympathy for businesses who get hacked, and you're wrongly labeled irresponsible, stupid.
- You may be questioned, possibly investigated, about **what you did to prevent this from happening**.
- You may need to **notify CLIENTS** that you exposed their data to cybercriminals, or at least were hacked, losing files and data, delaying projects and halting services.
- If the news (or your competitors) gets wind of this, they'll have a heyday, **destroying your reputation**.
- **Costs** for restoring data and work can quickly escalate.

RISK

STRATEGY

CompliancyIT

How Do You Protect Yourself?

CompliancyIT

Think Like A Cybersecurity Guy (or Gal)

The 5 Tenants of Zero Trust

- **Never Trust, Always Verify** – an email, a phone call, a text message, a DM
- **Assume Breach** – assume you have been or WILL BE breached
- **Assume a Hostile Environment** – don't trust anything, even if it says "secured"
- **Scrutinize Explicitly** – Doubt it, pick up the phone can call someone directly, look for signs that the communication is not authentic, if it doesn't feel right, don't trust it
- **Utilize Unified Analytics** – Corroborate the information you have and ASK FOR HELP

CompliancyIT

How To Protect Yourself

Vital Protection #1

Multi-Factor Authentication (MFA, 2FA)

CompliancyIT

How To Protect Yourself

Vital Protection #2

Up Your Password Game

Strong, Long, Unique

Password Manager

CompliancyIT

How To Protect Yourself

Vital Protection #3

Continuous Cybersecurity Awareness Training

Try to make it interesting, engaging and relevant

CompliancyIT

How To Protect Yourself

Vital Protection #4

Security Tools, the RIGHT ones

YOU CANNOT TOOL YOUR WAY SECURE

- EDR, MDR, XDR
- SIEM, SOAR
- SOC
- DLP
- Zero Trust Endpoint Protection, Application Whitelisting
- DNS Cleansing, Web Filtering
- VPN or SASE
- Firewall
- Spam Filtering/Email Security
- Removable media blocking
- Backup of critical data/apps

CompliancyIT

How To Protect Yourself

Vital Protection #5

Configuration Hardening

Devices, cloud platforms, applications

CompliancyIT

How To Protect Yourself

Vital Protection #6

Documentation

Policies, Plans, Procedures, Lists, Approvals, Ticketing

CompliancyIT

Secure Your Passwords Now:

"The Simple Guide To Hacker-Proof Passwords"

www.compliancyit.io/hackerproof

CompliancyIT

QUESTIONS?

Leia Kupris Shilobod, CSO & CEO
CompliancyIT
Author | Speaker | IT Princess of Power
Leia@compliancyit.io
www.compliancyit.io
724.235.8750.land
LinkedIn: /PrincessLeia
Signal: Leia Kupris Shilobod
Also found on Instagram and Facebook