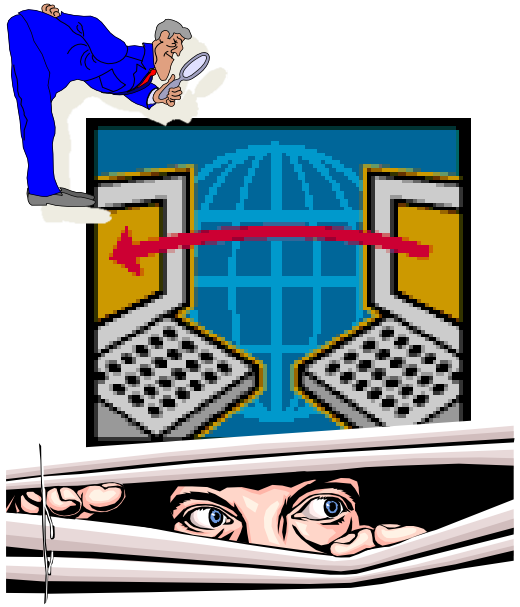
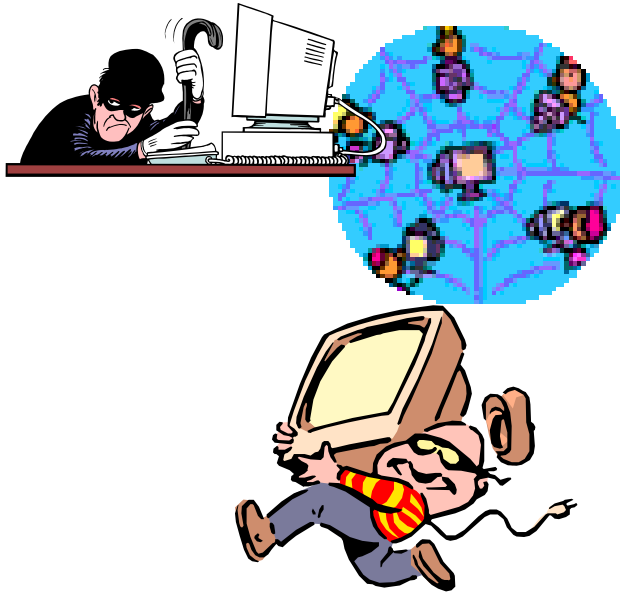
Cryptography And Network Security





Dr. E. Suresh Babu

Assistant Professor

Department of CSE

National Institute of Technology, Warangal

Erukala Suresh Babu

Digitally signed by Erukala Suresh Babu
DN: cn=Erukala Suresh Babu, o=NITW, ou=CSE, email=esbabu@nitw.ac.in, c=IN
Date: 2019.08.27 06:36:36 +05'30'

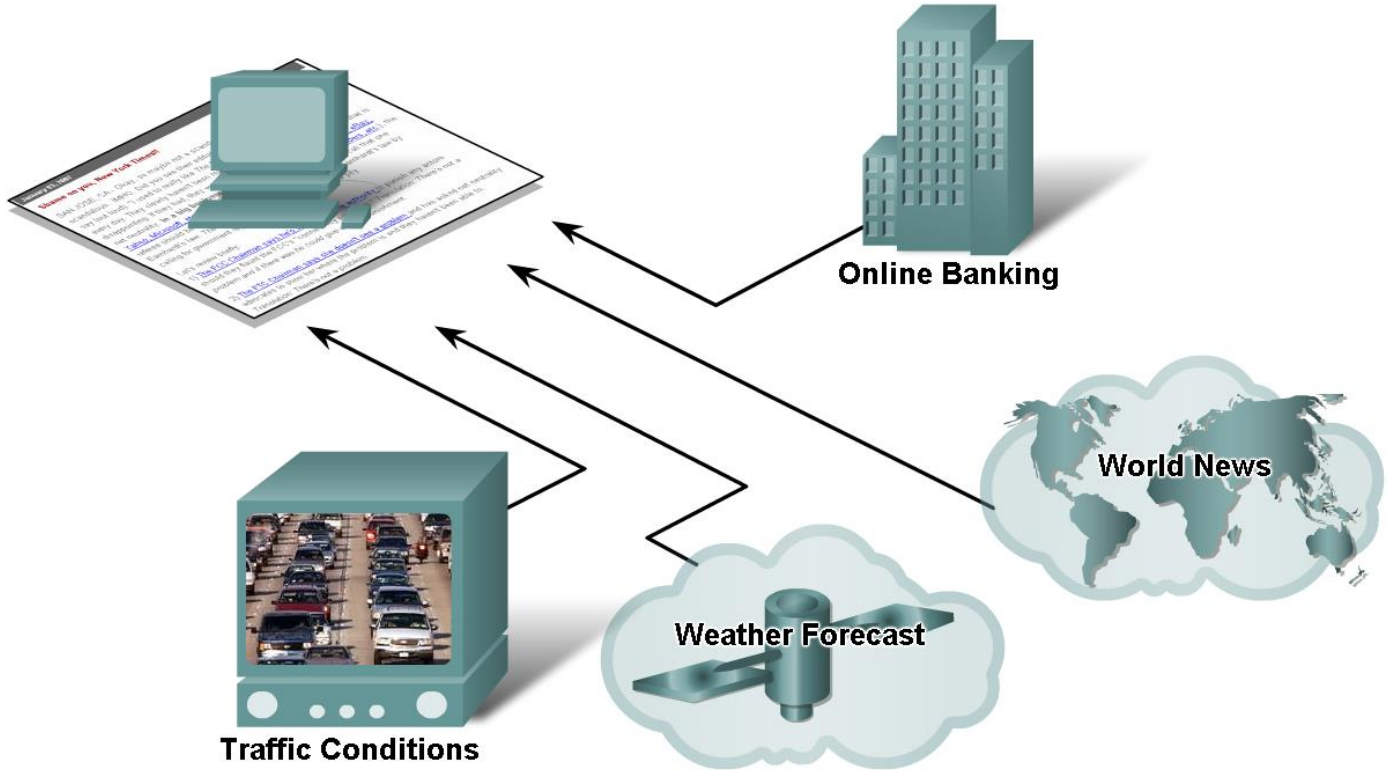
Session Outline

1. Networking(Internet) is Today's World
2. Trends and Technology
3. Trends of Attacks Against Technologies
4. Course Outline

Networking(Internet) is Today's World

How Networks Impact Daily Life

- Benefits of instantaneous communication and how it supports and improves our lives.

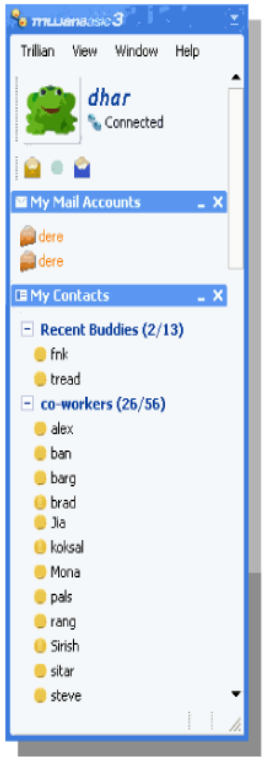


How Networks Impact Daily Life....

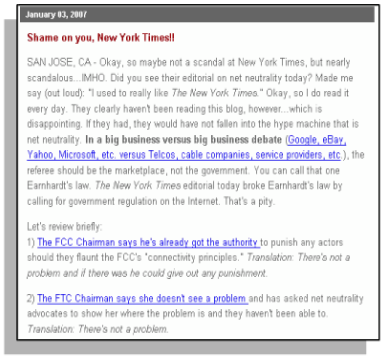
- Characteristics and **purpose of popular communication** media such as, **IM,**

Blogs, Podcasting, and Collaboration Tools

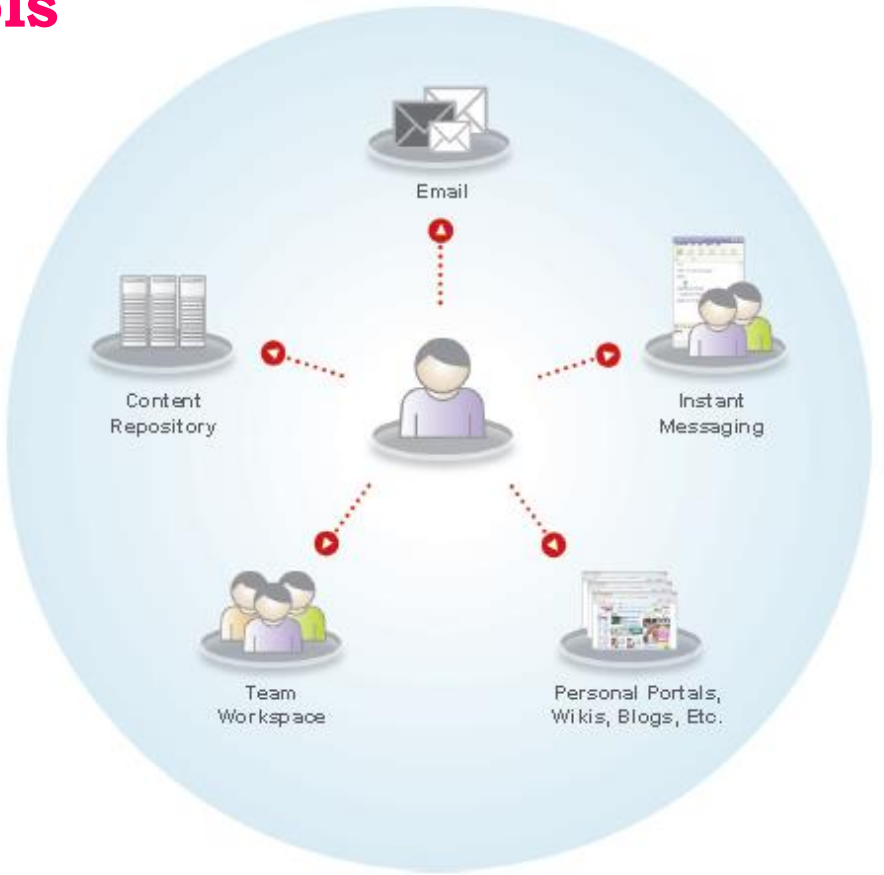
Instant Messaging



Weblog

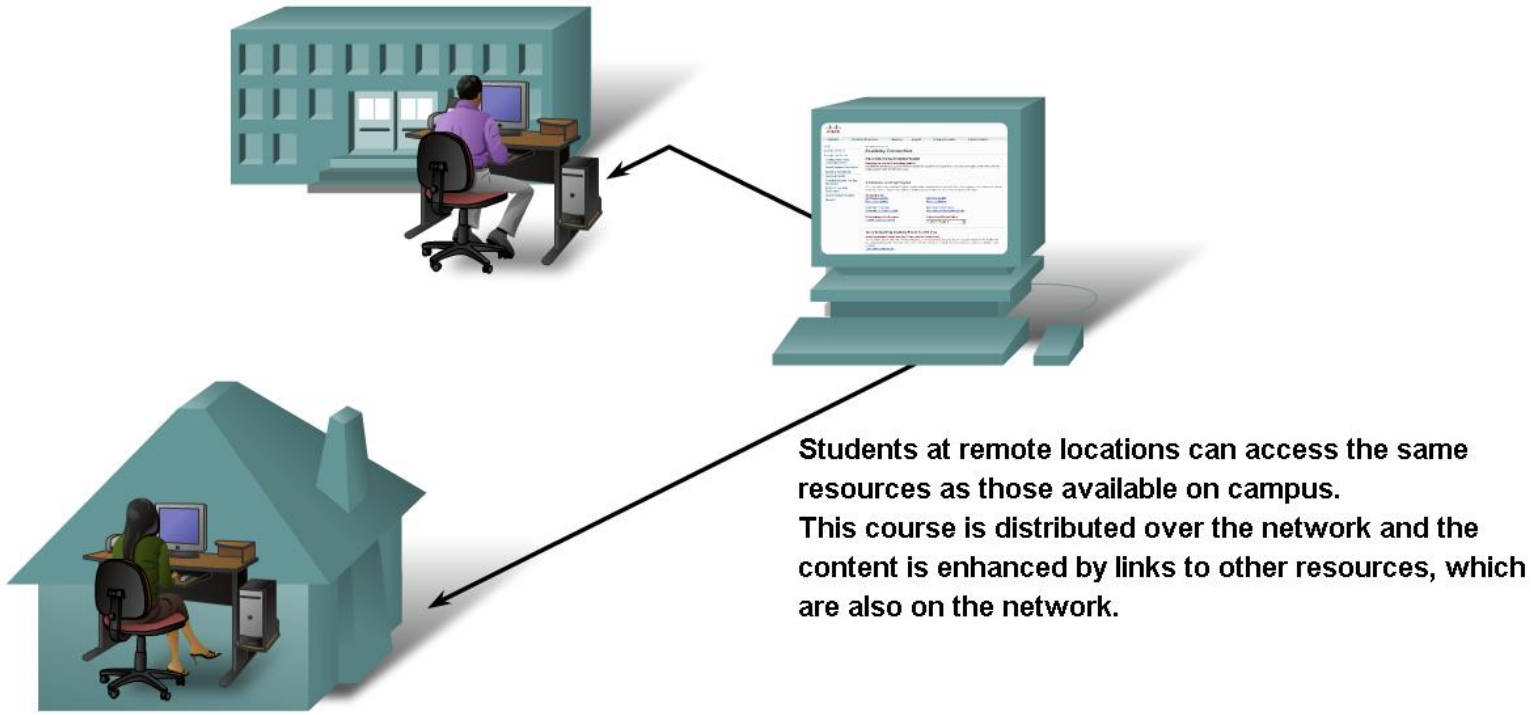


Podcasting



How Networks Impact Daily Life....

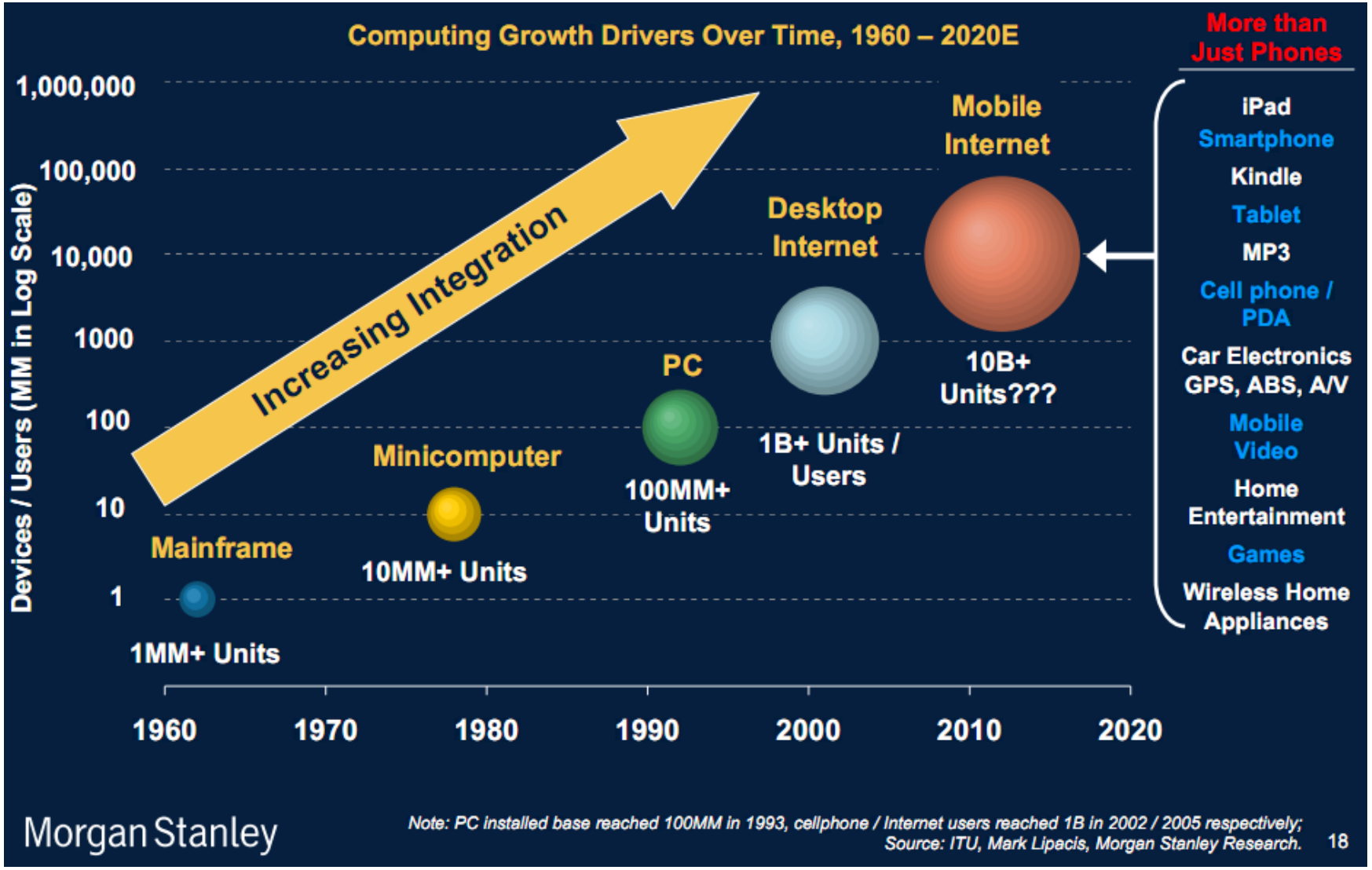
- Using information networks to share and collaborate improves teaching and learning



What Happens in an Internet Minute...

What Happens in an Internet Minute

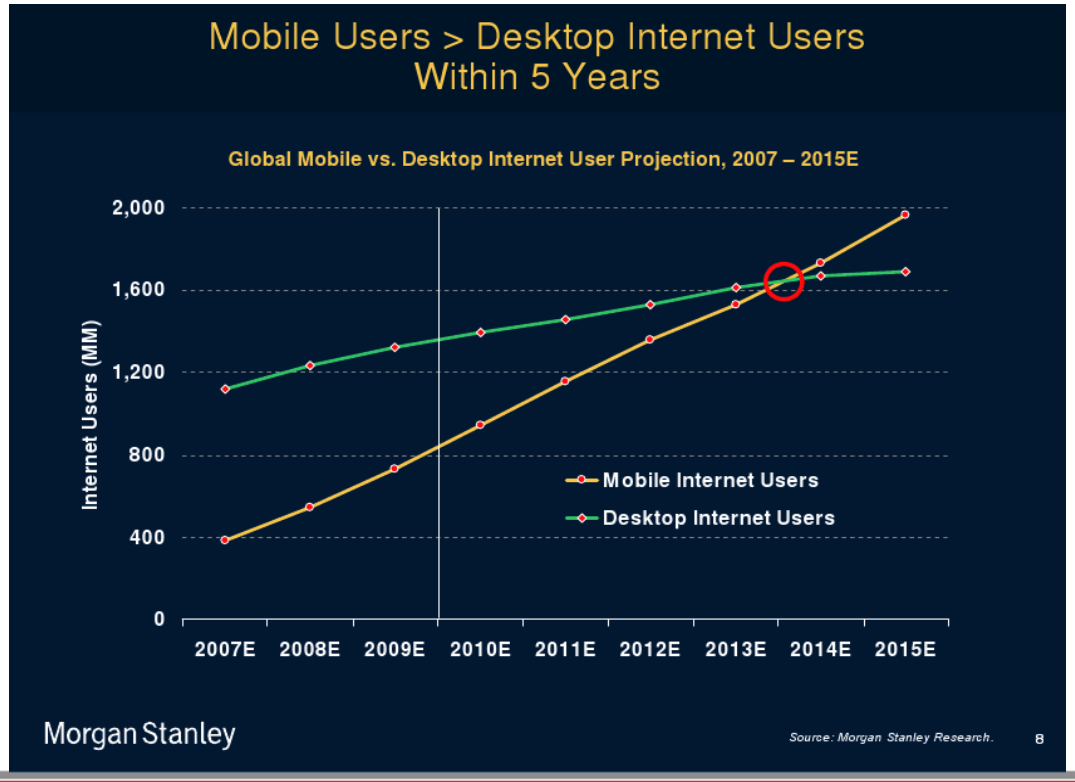
Where are we headed?



How do they get it?

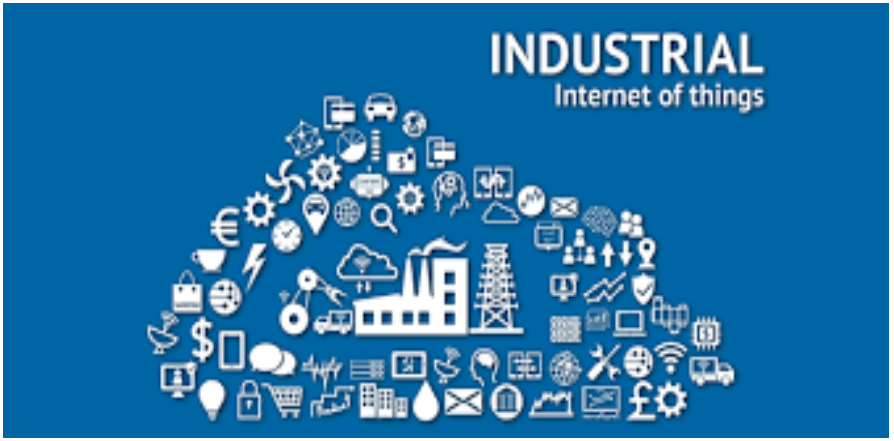
Mobile Traffic

Wireless and mobile traffic makes up **54% of global traffic**



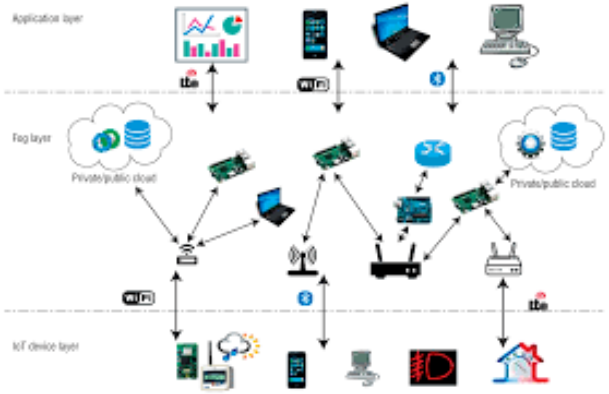
We Came A Long Way…

Applications Drive the Technology



Industrial IoT.

Big-Data



IoT/Edge Computing

“Cloudification”

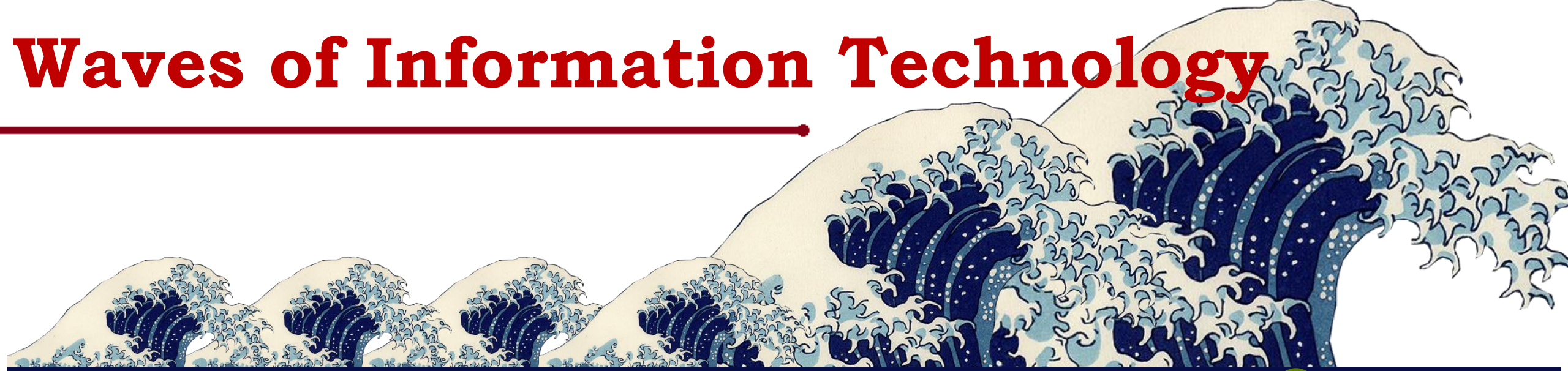
Robotics

Assisted Transportation.

Next Decade Technology

The Success of these Technologies

Waves of Information Technology



Mainframe	Mini	PC / Micro-processor	Networked/ Distributed Computing	IOT + Cloud + Big-Data	Cyber Security
Mid-'60s -'70s	*70s-80s*	*Late 70s-'90s*	*Mid-'90s-Today*		
IBM	DEC	Microsoft	Cisco		
Burroughs	IBM	Intel	Netscape		
Univac	DG	Apple	Google		
NCR	Wang	IBM	Microsoft		
Control Data	Prime	Sun	Oracle		
Honeywell	Apollo	HP	EMC		
NEC	…	Compaq	Salesforce.com		
…		…	. . .		

Future

Trends of Attacks Against Technologies

Cyber-attack is all too Real.

Cyber Criminals

Half of all cyberattacks are committed against **small businesses**.

Cyber Attacks

43 percent of cyber attacks are aimed at **small businesses**

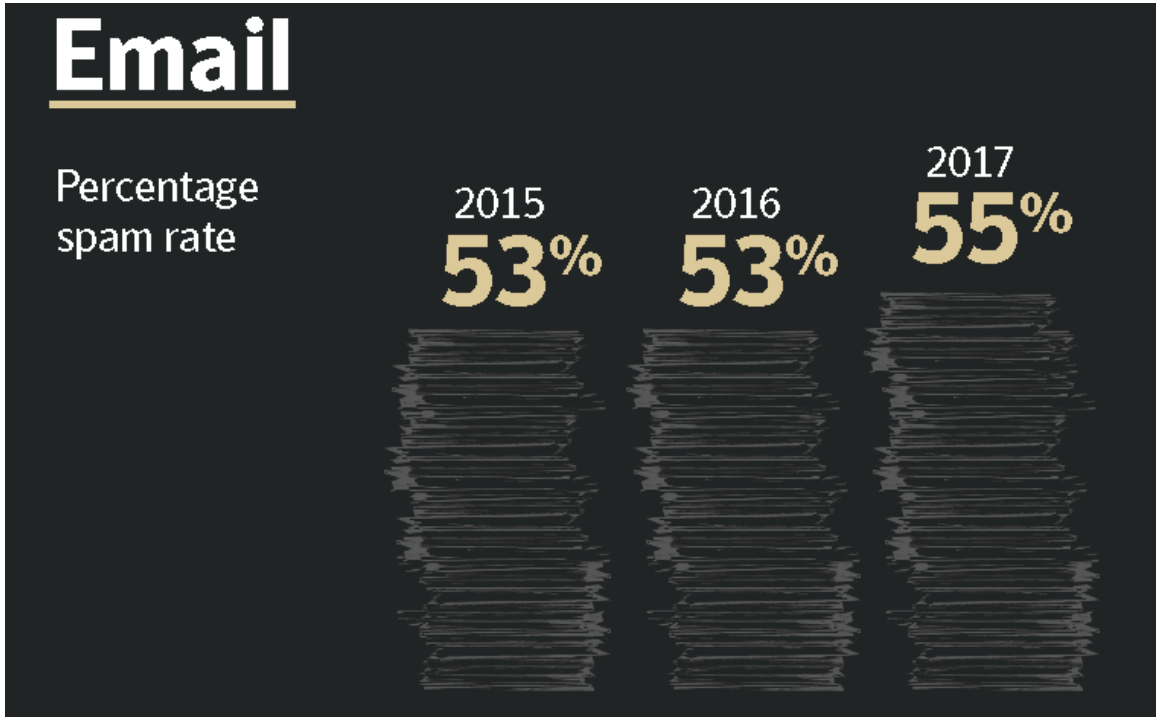
Crime

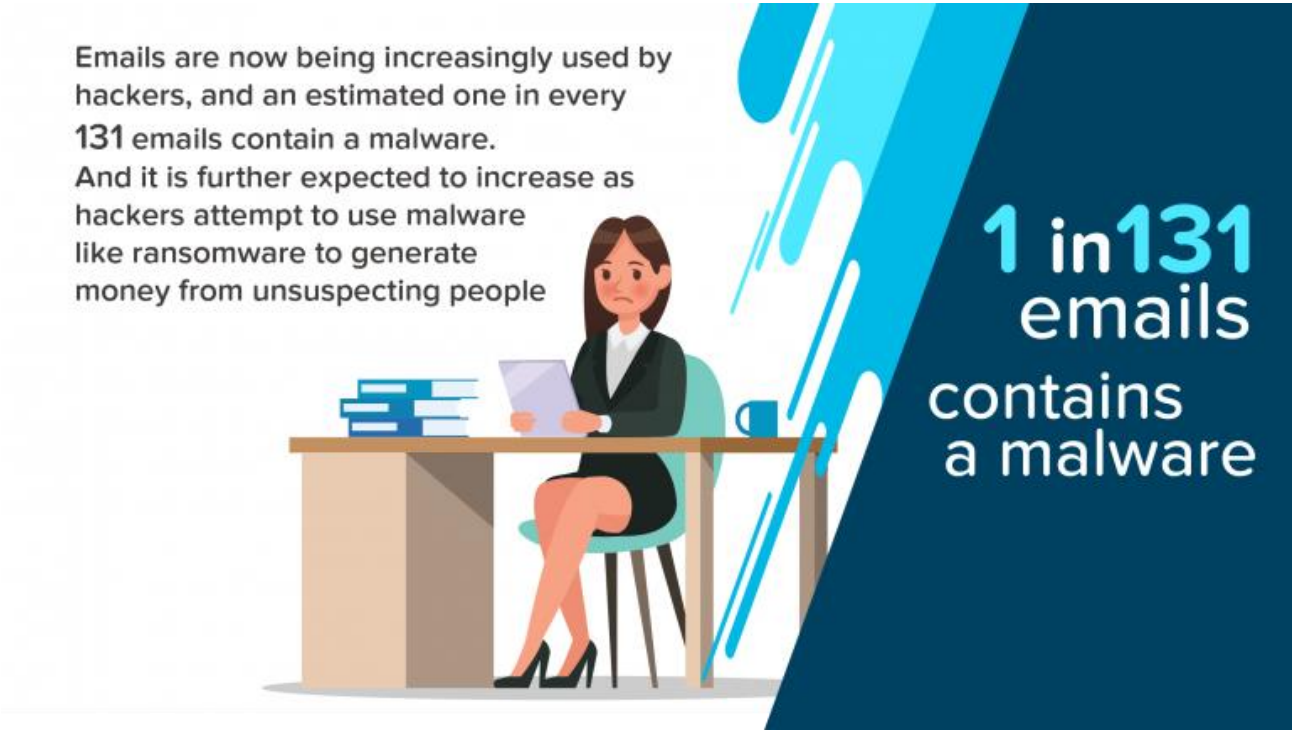
81 percent of data breach victims do not have a system in place to **self-detect data breaches.**

Warren Buffett

Cyber Attacks is the **BIGGEST threat to mankind** even more of a bigger threat than **nuclear weapons.**

Email Account





Malware


230,000
new malware samples
are produced every day
This is according to research from Panda Security, estimating Trojans to be the main source of malware — being responsible for about
51.45 percent of all malware


According to data from a researcher from the Erlangen-Nuremberg University, while many people claim to be aware of the risks of unknown links in emails, a good portion of them still click unknown links in emails
78
percent
of people
claim to know
the risks that
come with clicking
unknown links in
emails

Malware: Ransomware Attacks

Ransomware — a malware that **infects computers** and **restricts their access to files**, often threatening permanent data destruction unless a **ransom is paid.**

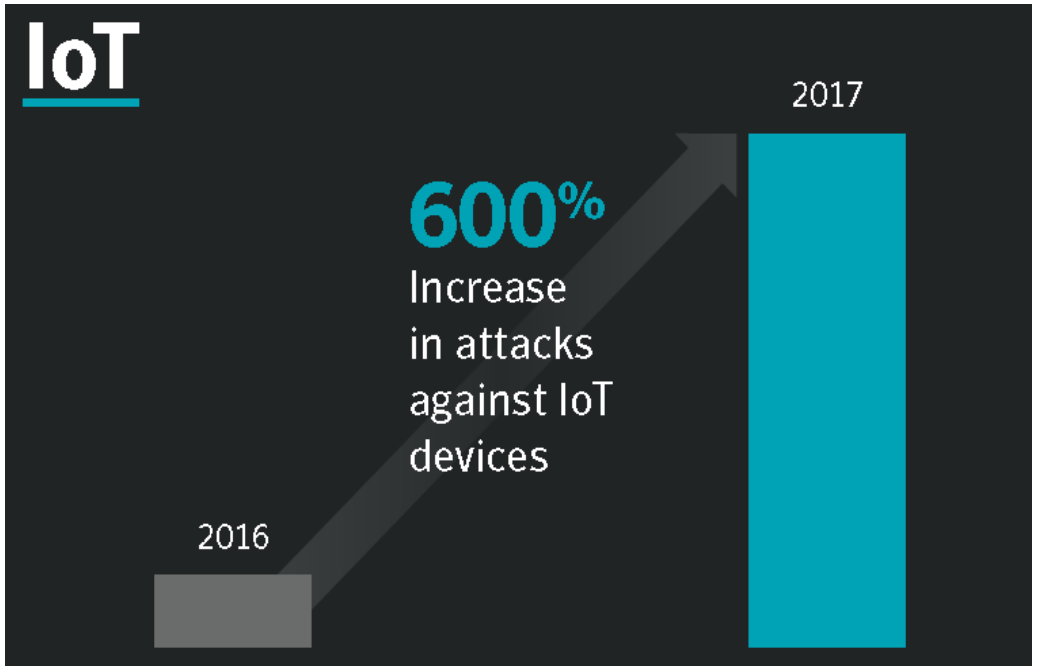
Malware: Ransomware Attacks

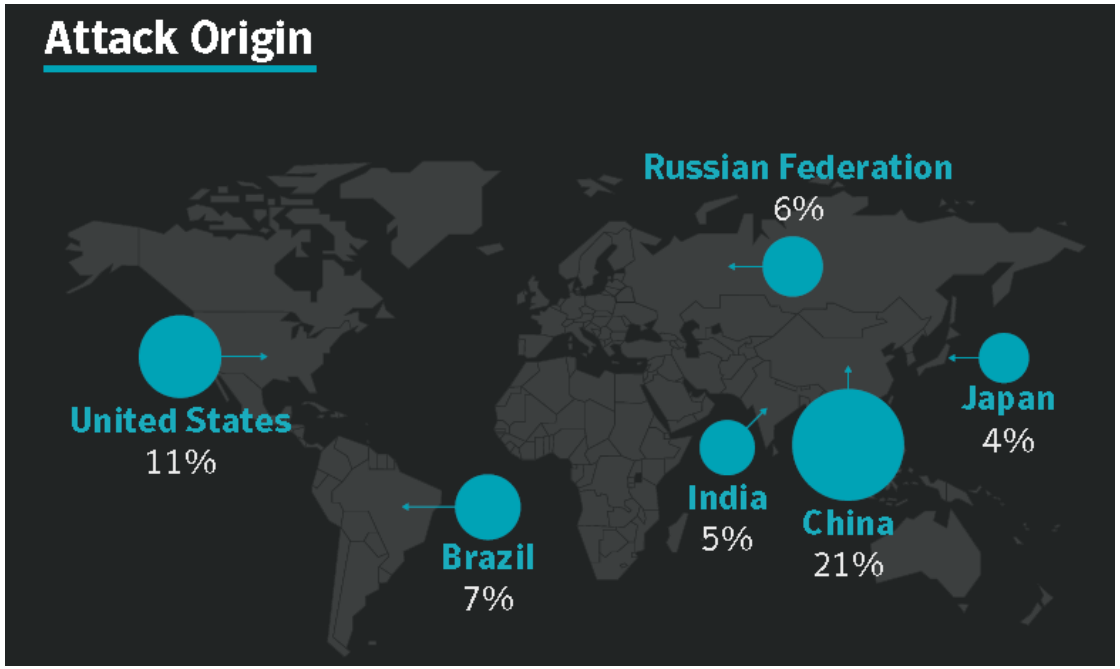
The **average amount demanded** after a ransomware attack is Rs **1,25,000.00.**

More than **4,000 ransomware attacks** occur every day.

Ransomware attacks increased by **42 percent in 2018.**

IoT Attacks


IoT
2017
600%
Increase
in attacks
against IoT
devices
2016


Attack Origin
Russian Federation
6%
United States
11%
Japan
4%
India
5%
China
21%
Brazil
7%

INSIDER THREAT

Inside Threats

Today's most damaging security threats are not originating from malicious outsiders or malware but from trusted insiders - both malicious insiders and negligent insiders

Most Vulnerable To Insider Attacks?

What type(s) of insiders pose the biggest security risk to organizations?*

56%
Regular employees

55%
Privileged IT users/admins

42%
Contractors/service providers/ temporary workers

Privileged business users/ executives

Customers/ clients

None

Not sure/ other

IT Assets At Risk

57% Confidential business information
(Financials, customer data, employee data)

52%
Privileged account information
(Credentials, passwords, etc.)

49%
Sensitive personal information
(PII/PHI)

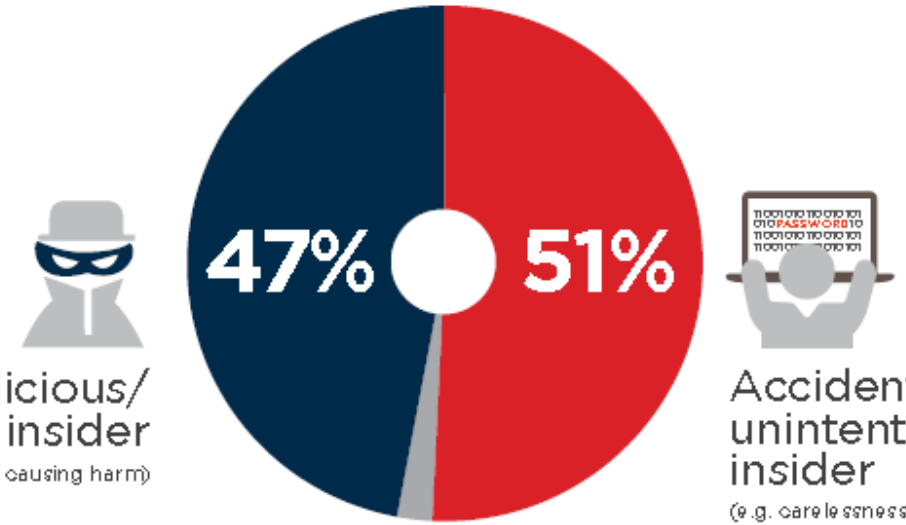
32%
Intellectual property
(Trade secrets, research product designs)

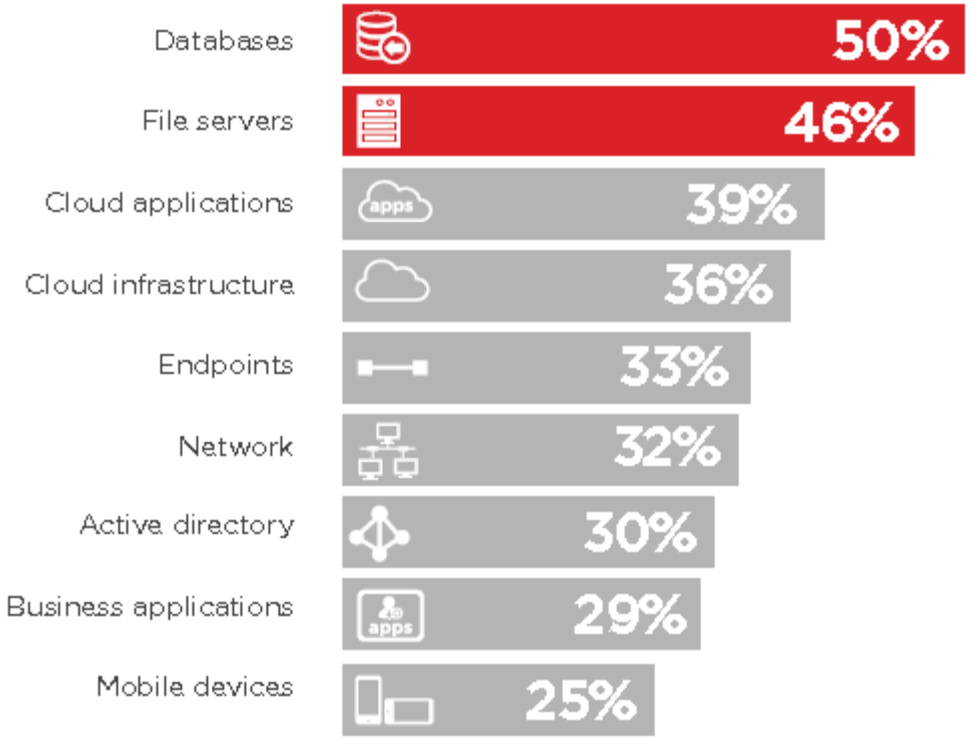
31%
Employee data
(HR)

27%
Operational/ infrastructure data
(Network, infrastructure controls)

Not sure/other 1%

What Type of Insider Threats



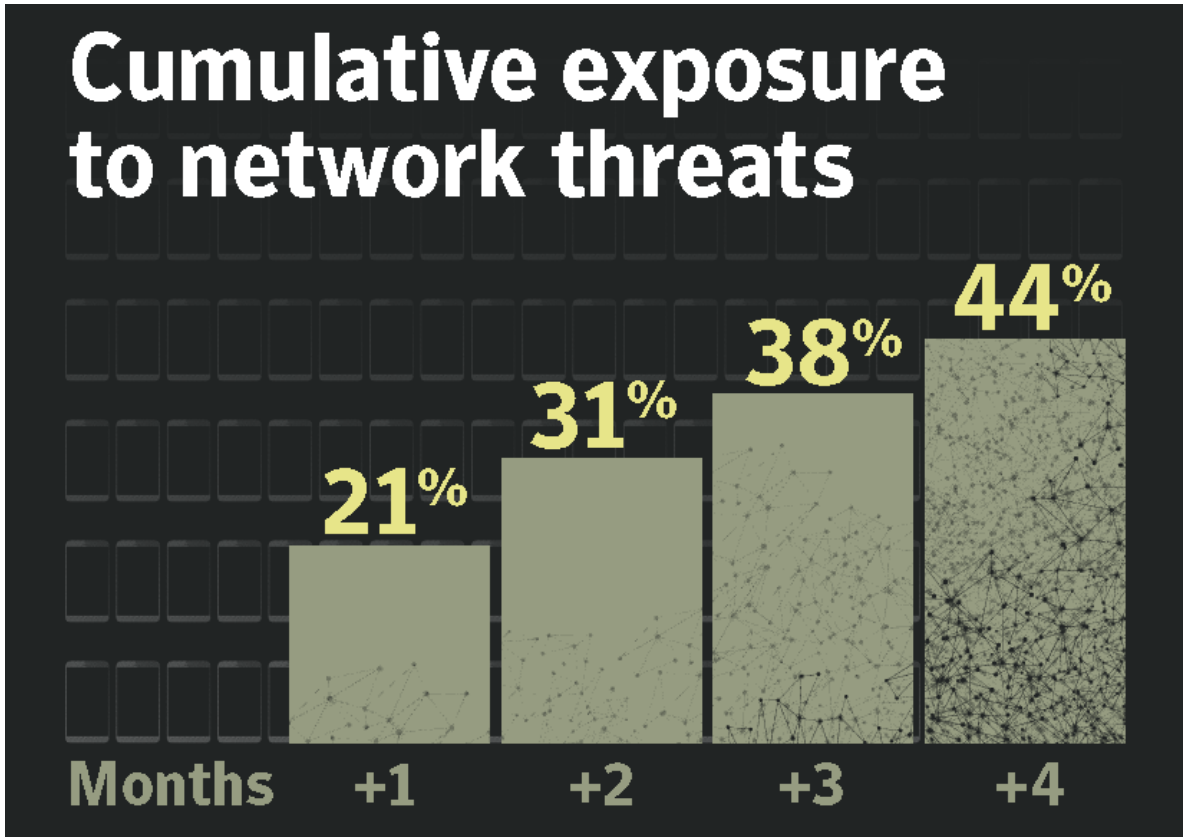


How Cybercriminals use Stolen Data

Cybercriminals are constantly trying to steal data and identities:

Personal Data Stolen

- ✓ Usernames
- ✓ Date of birth
- ✓ Passwords
- ✓ Credit card numbers
- ✓ Account numbers
- ✓ Employment information



Accidental Insider Threats?

67% Phishing attempts

56%
Weak/reused passwords

44%
Unlocked devices

44%
Bad password sharing practice

32%
Unsecured WiFi netwo

37%

Too many users with excessive access privileges

36%

Increasing number of devices with access to sensitive data

35%

Technology is becoming more complex

34%

Increasing amount of sensitive data

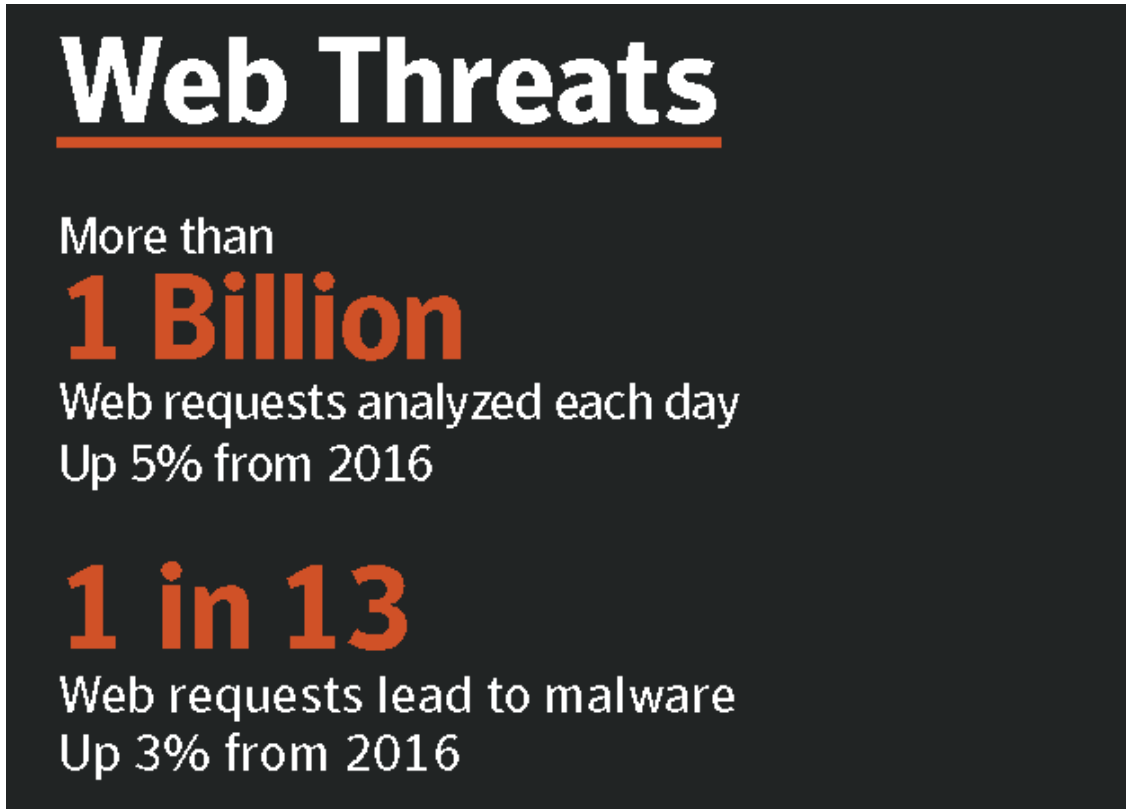
31%

Lack of employee training/awareness

Web Threats

Dark Web

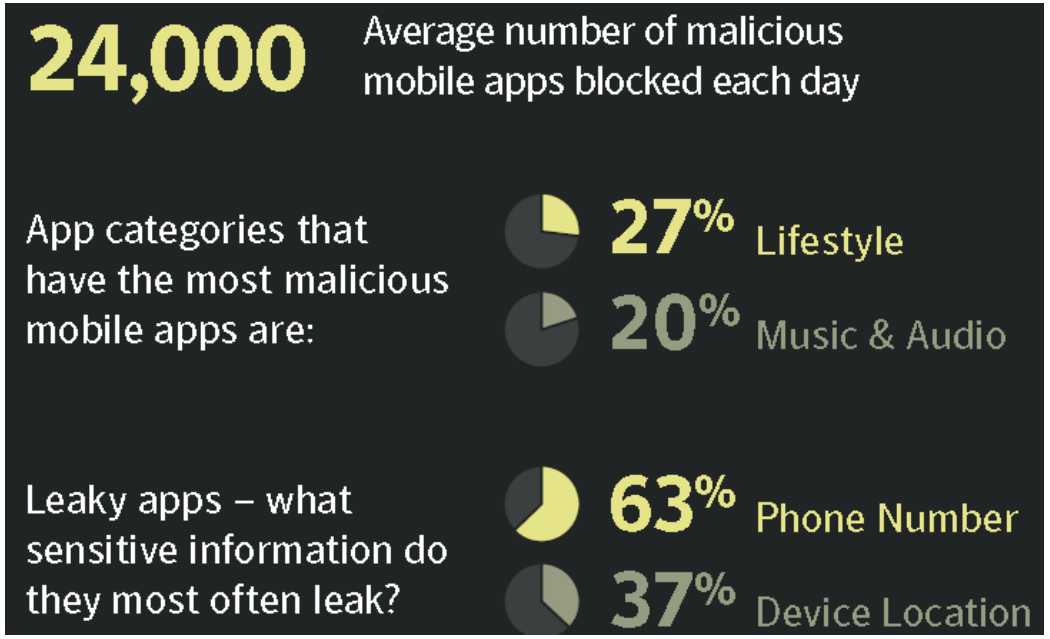
Deep Web or Dark Web — are intentionally hidden and used to **conceal and promote heinous criminal activities.**

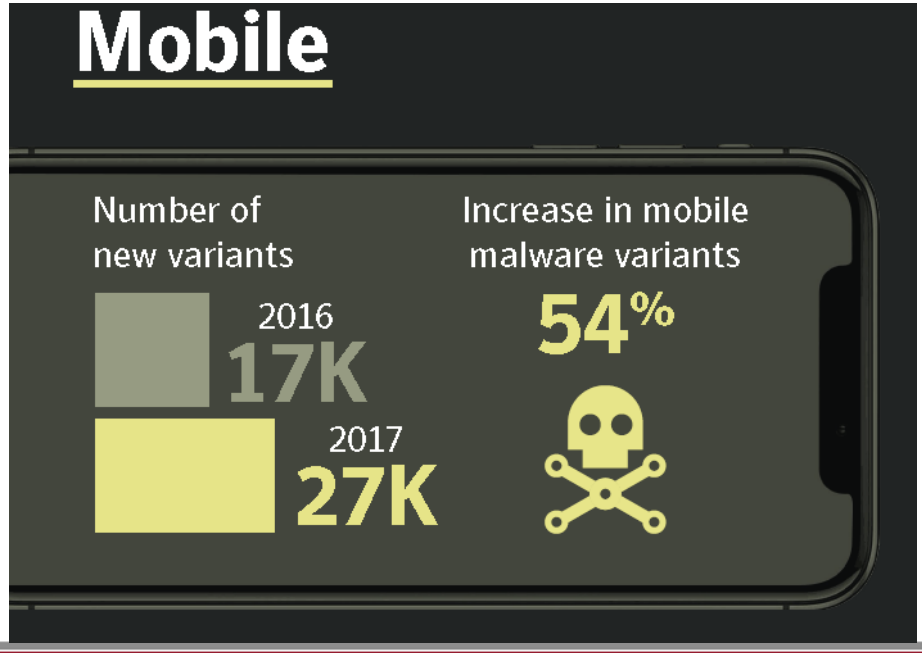


Mobile Threats

Mobile Malware continues to surge Threats in the mobile space continue to **grow year over year.**

Android is the second most **targeted platform by hackers** after Windows.





Wireless Devices

The **world's digital content** is expected to grow from **4 billion zettabytes last year to 96 zettabytes by 2020**

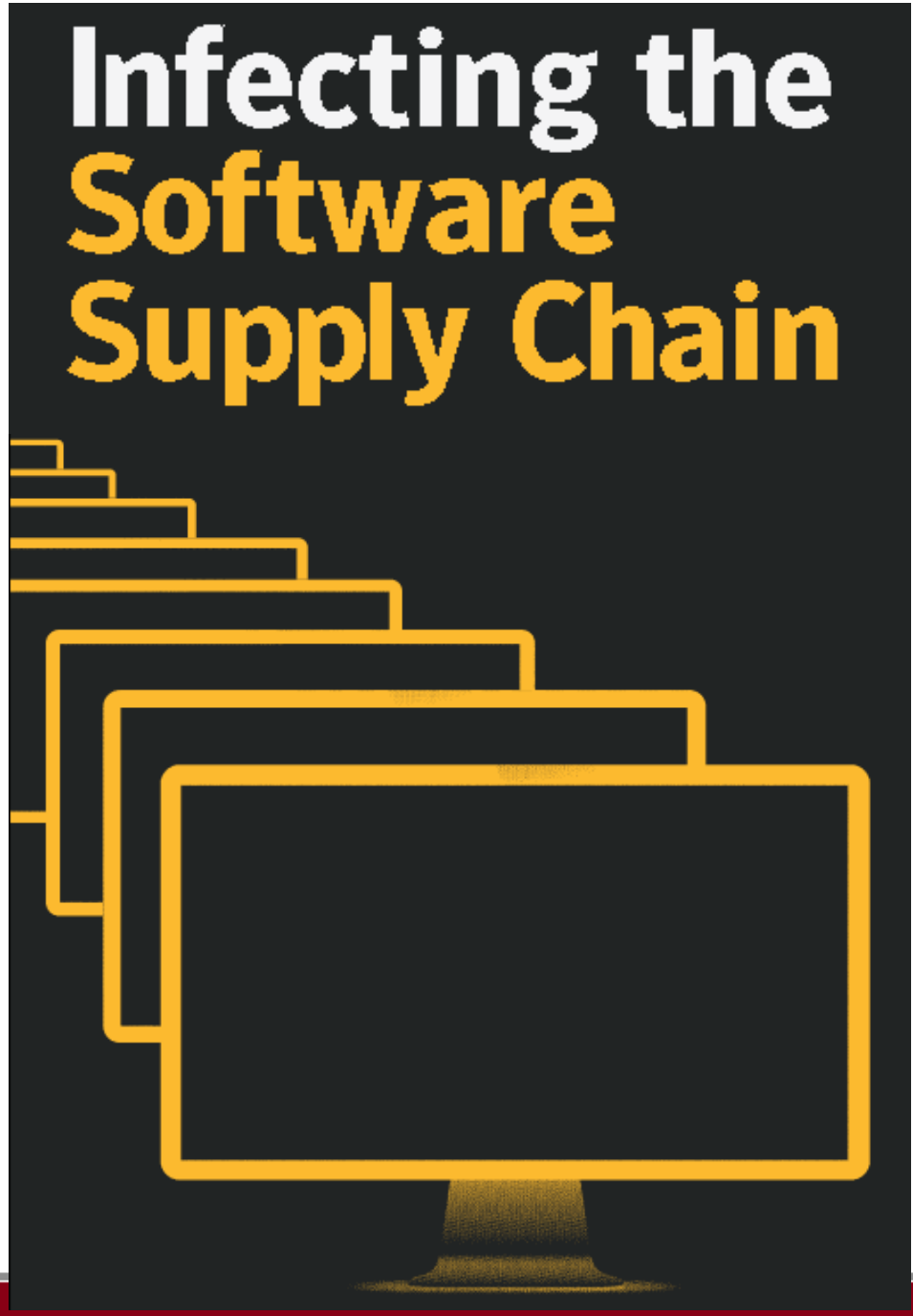
Hundreds of thousands — and possibly millions — of people can be **hacked now via their wirelessly connected** and digitally monitored

Gartner

Forecasts more than **half a billion wearable devices** will be **sold worldwide in 2021,** up from roughly **310 million in 2017.**

Software Threats

- There are **111 billion lines of new software code** being produced each year — which introduces a **massive number of vulnerabilities** that can be exploited.



Course Outline

Course Description

- The course covers **theory and practice of Network Security**, focusing in particular on the **security aspects of the Computer Network.**

Course Description

- This course introduces some **basic cryptographic tools** to provide security, such as
  - ✓ **Shared Key Encryption (DES, 3DES, RC-5, etc.);**
  - ✓ **Public Key Encryption**
  - ✓ **Key Exchange**
  - ✓ **Digital Signature (Diffie-Hellmann, RSA, DSS, etc.).**

Course Description

- This course also provides how **cryptographic tools are utilized** in the **internet protocols and applications** such as **SSL/TLS, IPSEC, Kerberos, PGP, S/MIME, SET**, and others (including wireless).
- Finally, **system security issues**, such as **Viruses, Intrusion, And Firewalls,** will also be covered.

Course Objective

- Students learns
  - ✓ Learn fundamentals of **cryptography and its application** to network security.
  - ✓ Understand **network security threats, security services, and countermeasures.**
  - ✓ Acquire background on well known **network security protocols such as IPSec, SSL.**
  - ✓ Acquire background on **hash functions; authentication; firewalls; intrusion detection techniques.**
  - ✓ Gain **hands-on experience** with programming and simulation techniques for **security protocols.**

Your Role : Think Like an Engineer

- What technologies should be employed to build a security within network
- Develop interest in performing research in the area of Networks Security

Course Outcomes (CO)

- Students will able to

1. **CO1 : Analyze encryption algorithms.**
2. **CO2 : Perform packet sniffing and analyze packets for vulnerabilities**
3. **CO3 : Identify system vulnerabilities of communication protocols**
4. **CO4 : Design firewalls**
5. **CO5 : Develop intrusion detection system**

Course Logistics

1. William Stallings, Cryptography and Network Security: Principles and Practice, 5th Edition, Pearson Education, Fifth Edition, 2011
2. William Stallings ,Network Security Essentials: Applications And Standards Edition-Fourth Edition-2011
3. Eric Cole, Dr. Ronald Kurtz and James W. Conley, Network Security Bible, Wiley Publishers, 2009
4. Jason Albanese and Wes Sonnenreich, Network Security Illustrated, MGH Publishers, 2003

Where to find me

Instructor : **Dr. E.SURESH BABU**

E-Mail : **esbabu@nitw.ac.in**

Website : **www.nitw.ac.in**

Office Hours : **9.00 A.M – 5:30 P.M**

My Office : **E-ICT Block, Ground Floor, Room No : 104**

Course Work

1. **Minor Tests (Two Tests) -- 20 Marks**
2. **Mid Semester Examination – 30 Marks**
3. **End Semester Examination – 50 Marks**

All the Best

Thank U