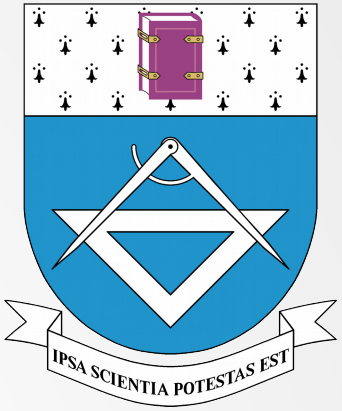
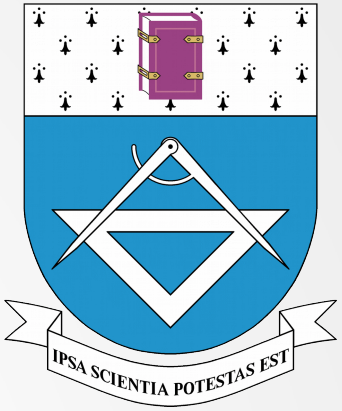


People – the last line of defence in cybersecurity?

Cristian-Mihai Amarandei, B.Eng. (Hons), PhD

cristian.amarandei@tuiasi.ro



People – the first line of defence in cybersecurity?

Cristian-Mihai Amarandei, B.Eng. (Hons), PhD

cristian.amarandei@tuiasi.ro

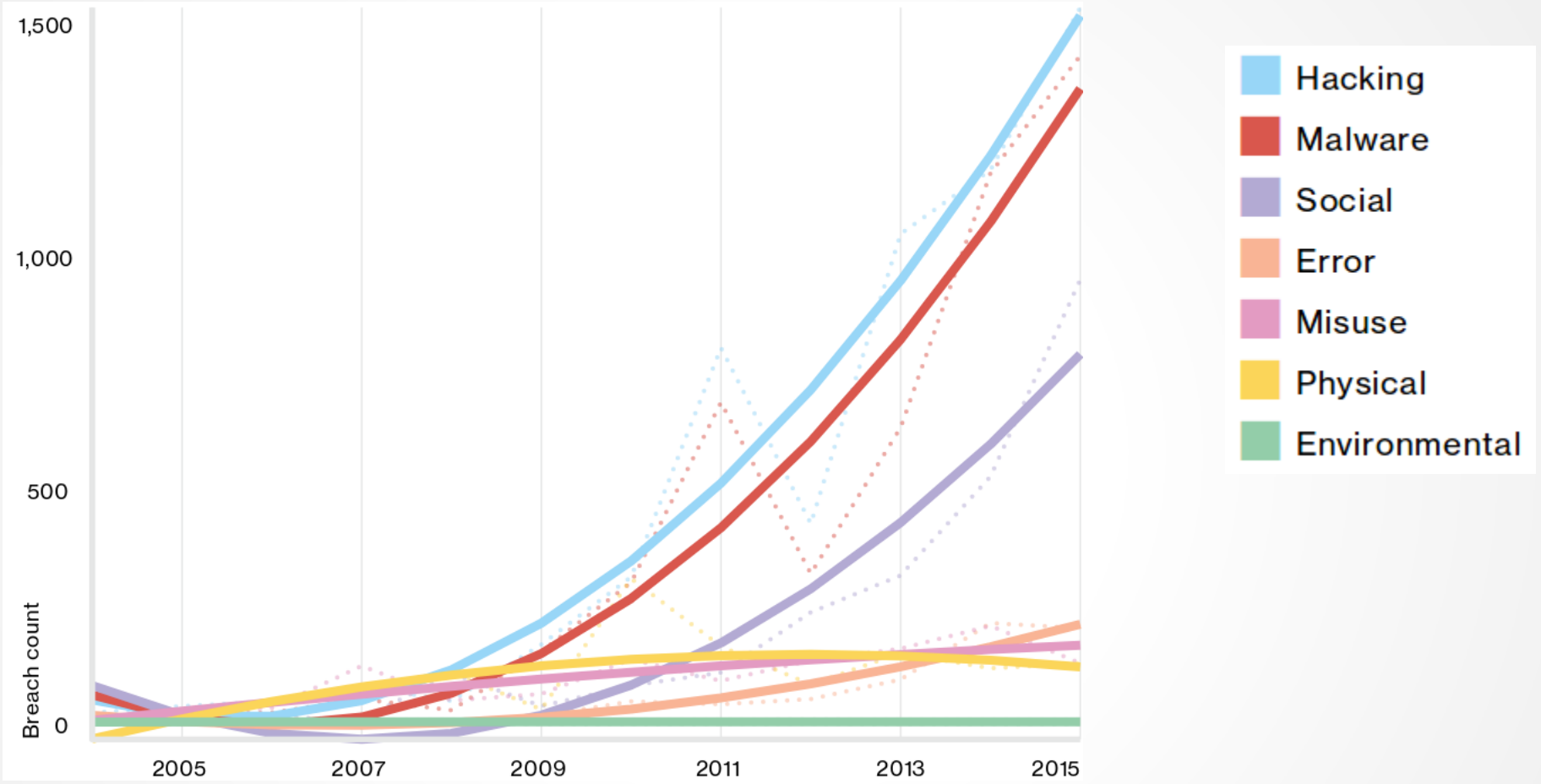
Motivation to break into systems

- Industrial espionage
- Financial gain
- Revenge (disgruntled actual/former employees)
- Status
- ...

Threats to Network Security

- Hackers
- Disgruntled employees
- Organizations: suported by some governements as spying technique, organized crime, terorrists
- Virues, trojan program, malware ...
- Social engineering: - the people factor
- ...

Verizon 2016 Data Breach Investigations Report



What can we secure?

- The network
  - Block potential attackers and known means of attack
  - secure connectivity with trusted users
- Activities that require secure connectivity
  - Remote access to the internal network
  - Access to applications and services (e-mail, web …)

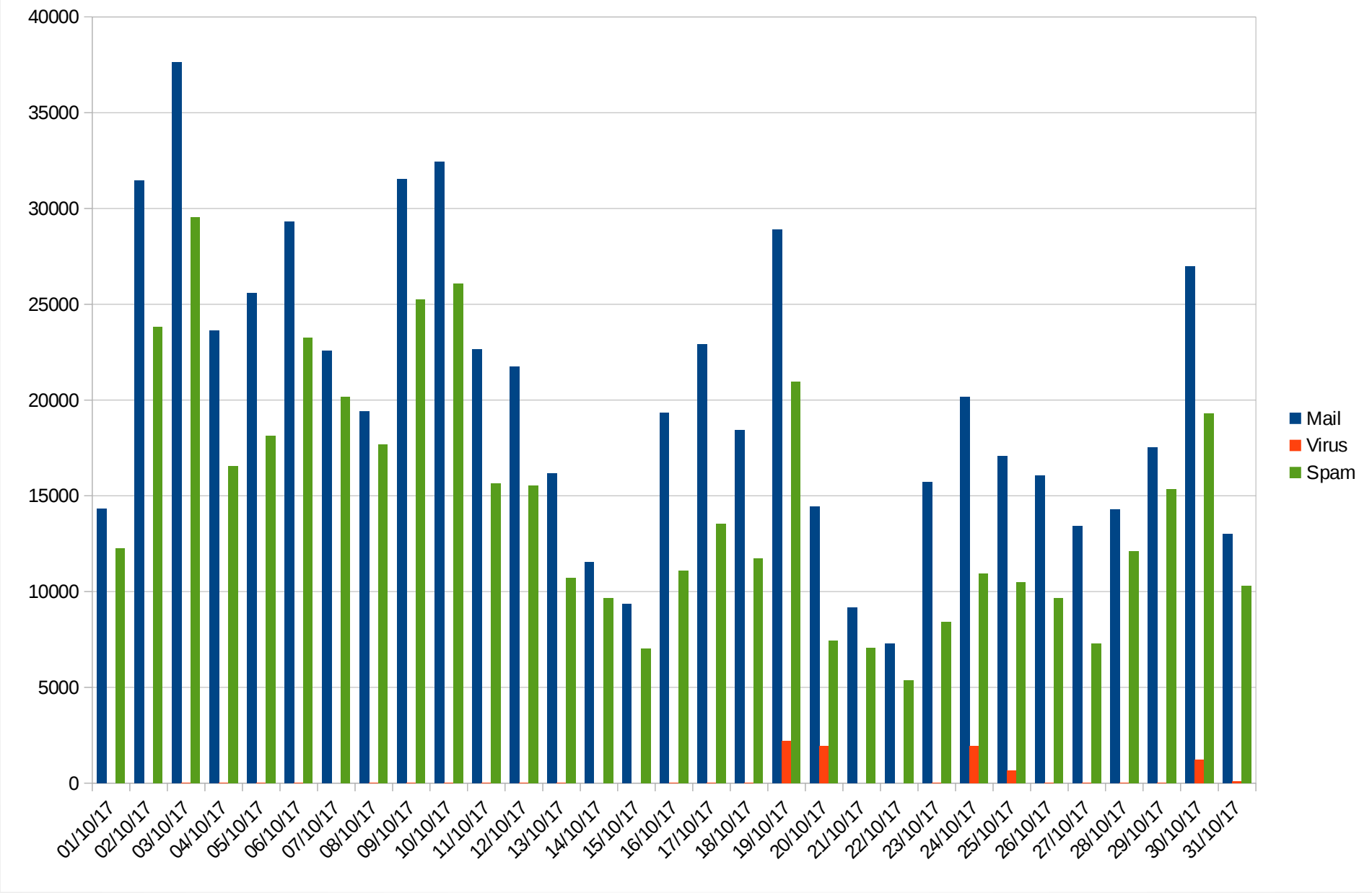
Social Engineering: the people factor

- Attackers can try to gain access through users
  - Employees can be tricked to provide data access to resources
- **Protect the end-user**
  - Organizations need a security policy and rigorous training program

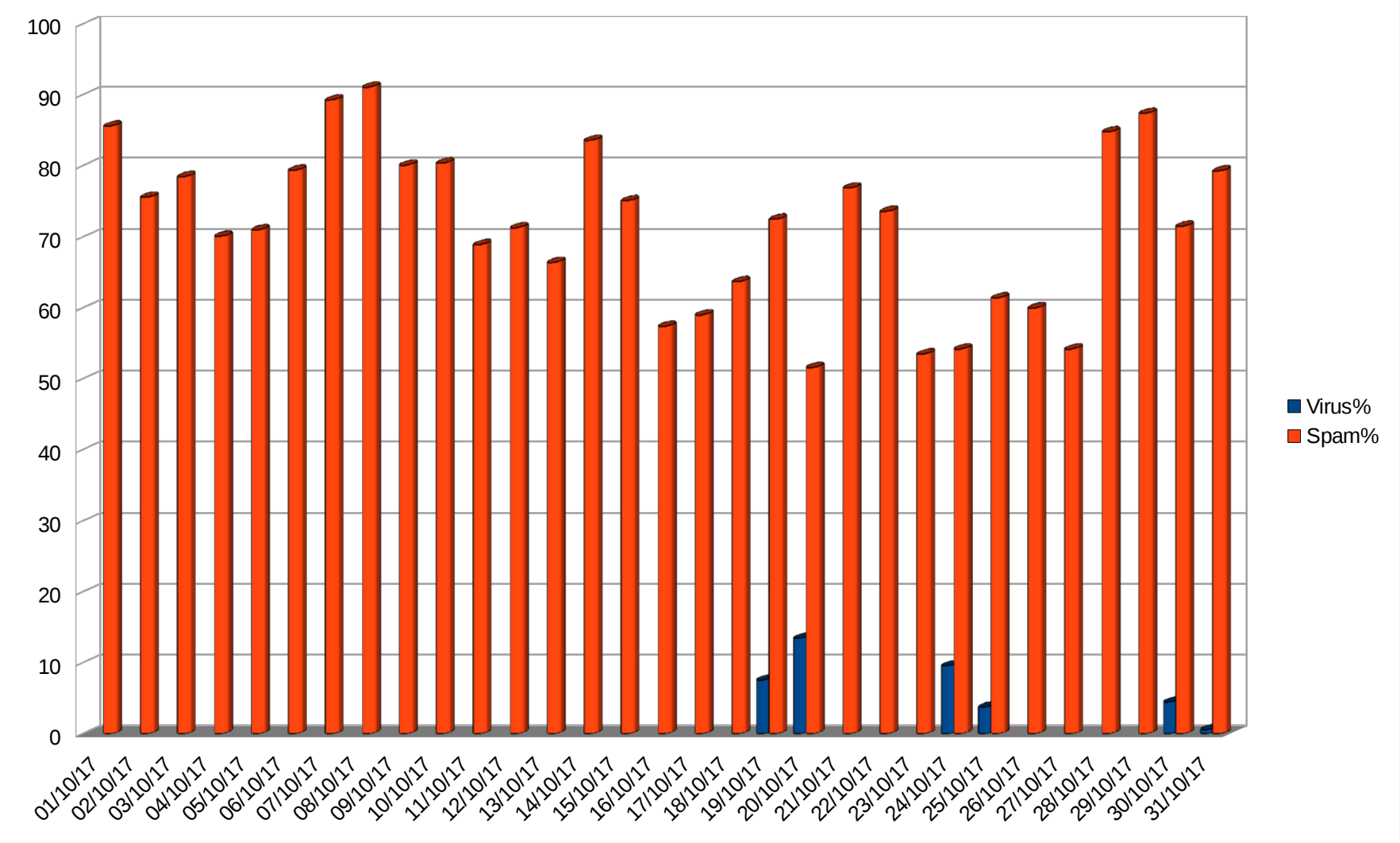
how ?

- Security Policies / Usage guidelines
- Purchase of specialized equipment and software
- **Educate the end-user !!**

Spam detected in e-mails



Some more details ….



- Total number of messages – 624,022
- Detected spam 452,163 – **72,5%**

after spam detection and delivery of messages ..

- How many of the messages detected as spam contained possible attack vectors?
- How many of the messages that passed the detection system had potential attack vectors?
  - Where and from what devices have messages been read?
  - What did the user do?

Security policy

- Is necessary if
  - employees work with confidential information
  - data loss could result in severe financial loss
  - organization has trade secrets
  - the internet is used daily
  - organization is subject to regulation for information security and privacy (**GDPR** !)

Security Policy

- Gives users guidelines on how to handle sensitive information
- Gives IT staff instructions on what defensive systems to configure
- Reduces the risk of legal liability
- A good security policy is comprehensive and also flexible
  - Is a group of documents instead of a single document

Security policy

- too complex – no one will follow
- fails if affects productivity
- should state clearly what can and cannot be done in the organization network or on equipment and property
- must include generalized clauses
- people need to know why the security policy is importat
  - and specific consequences for violating the policy !!

Security policy

- **must involve representatives of all departments**
- needs support from the highest level of the company management
- employees must sign a document acknowledging the policy and agreement to abide by it
- updated with current technologies and consistent with applicable laws

How do we know if the policies are well done?

- International standards and guidelines are available
  - ISO/IEC 27002:2013
  - Payment Card Industry Data Security Standard (PCI DSS) - https://www.pcisecuritystandards.org
  - National Institute of Standards and Technology (NIST) Cybersecurity Framework - https://www.nist.gov/cyberframework
  - IASME - https://www.iasme.co.uk/

What about the end-user?

- All employees / users must be educated about security dangers and security policies
  - **rigorous training program !!**
- Employees are most likely to detect security breaches
  - or then cay cause one (accidentally !?)
  - they can observe suspicious activities
- **Enforcing** the security policy !!

People – the first or the last line of defence?