Impact of Cyber Threats on Business Profitability

Dr. Mohsen Gerami

Head of Computer and Information Technology Department of ICT Faculty

ITU CENTRES OF EXCELLENCE NETWORK FOR ASIA-PACIFIC REGION

ITU- ICT Faculty training on "Cybersecurity" 12-16 May 2018 - Tehran, Islamic Republic of Iran

Agenda

- Introduction
- The importance of the subject
- Research Questions
- Why cyber security needs to be a topic of boardroom agenda?
- Cyber Insurance
- Reducing Cyber risk
- Increasing Cyber Security
- Business cyber security plan
- Research achievements

Introduction

- Cyber attacks can be labelled as either a cybercampaign, cyberwarfare or cyberterrorism in different context.
- a large number of companies have been the victims of these cybercrime attacks, which greatly affect their profitability.
- Cybercrime is the greatest threat to every company in the world, and one of the biggest problems with mankind.
- Cyber security Ventures predicted that cybercrime will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015.
- This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, and will be more profitable than the global trade of all major illegal drugs combined.

Introduction

- In 2017, WikiLeaks reported recently, the CIA lost control of the majority of its hacking arsenal including malware, viruses, trojans, weaponized "zero day" exploits, malware remote control systems and associated documentation.
- "Year Zero" introduces the scope and direction of the CIA's global covert hacking program, its malware arsenal and dozens of "zero day" weaponized exploits against a wide range of U.S. and European company products, include Apple's iPhone, Google's Android and Microsoft's Windows and even Samsung TVs, which are turned into covert microphones

Introduction

- Theft of information from companies on the one hand and cybercrime attacks such as DDoS to their servers have greatly affected the profitability of these companies.
- Distributed Denial of Service (DDoS) attacks generate enormous packets by a large number of agents and can easily exhaust the computing and communication resources of a victim within a short period of time.
- DDoS attacks are constantly evolving as the nature of technology used and the motivations of the attackers are changing.
- Even today, perpetrators are being caught and charged with DDoS attacks launched via botnets that cause tens of thousands of dollars of damage to the victims

Research Questions

1) What is the benefit of having a cyber-security debate in the board meetings of an organization?
2) What can justify these costs, given the cost of cyber security in the organization?
3) If the organization's profitability is targeted despite the use of cyber-security in the organization, what can be the best solution for the organization?
4) What is the significance of a cyber-security plan for the profitability of an organization?

The importance of the subject

- In 2017, in two steps, very important information was disclosed from the heart of the United States government.
- WikiLeaks firstly unveiled Vault7 in March, revealing widespread information about the hacking and infiltration of the CIA in its victim's computer.
- At a later stage and in April of 2017, the Shadow Breakers hacker group revealed a wealth of hacking tools from the National Security Agency (NSA).
- Both of these disclosures have greatly influenced the security of cyberspace and the concerns of experts in this field.
- This created a threat to the credibility of many large companies.

The importance of the subject

- Companies also frequently fail to patch security flaws in a timely manner.
- In particular, ransomware -- when hackers demand money to unlock files -- is becoming more common.
- An analysis from anti-virus software firm Bitdefender found ransomware payments hit $2 billion in 2017, twice as much as in 2016.
- Meanwhile, Trend Micro predicts global losses from another growing trend, compromised business email scams, will exceed $9 billion next year

The importance of the subject

- Another risk that threatens businesses and organizations is the penetration of organizational networks with its devastating impacts.
- Today’s information systems face sophisticated attackers who combine multiple vulnerabilities to penetrate networks with devastating impact.
- The overall security of an enterprise network cannot be determined by simply counting the number of vulnerabilities.
- To more accurately assess the security of enterprise systems, one must understand how vulnerabilities can be combined and exploited to stage an attack

The importance of the subject

- One of the most serious threats facing business organizations is DDoS attacks.
- Denial-of-service attacks are characterized by an explicit attempt by attackers to prevent legitimate use of a service.

Why cyber security needs to be a topic of boardroom agenda?

- Countless cyber-attacks have shown us that an incident can have catastrophic consequences.
- For a business, this can lead not just to the loss of data, but also to expensive and time-consuming production delays, and, in the worst-case scenario, an entire business shutting down with a serious impact on the brand and its reputation.

Why cyber security needs to be a topic of boardroom agenda?

- As the potential impacts of cybersecurity threats increase, business leaders know that they must take these threats seriously.
- The Chief Information Security Officer (CISO) provides leadership and guidance to ensure that an organization can manage cybersecurity risks to its critical assets

Why cyber security needs to be a topic of boardroom agenda?

- Organizations are struggling to worry about cyber-security at the board level to ensure that their information assets are protected and that they are less likely to attack cyber security.

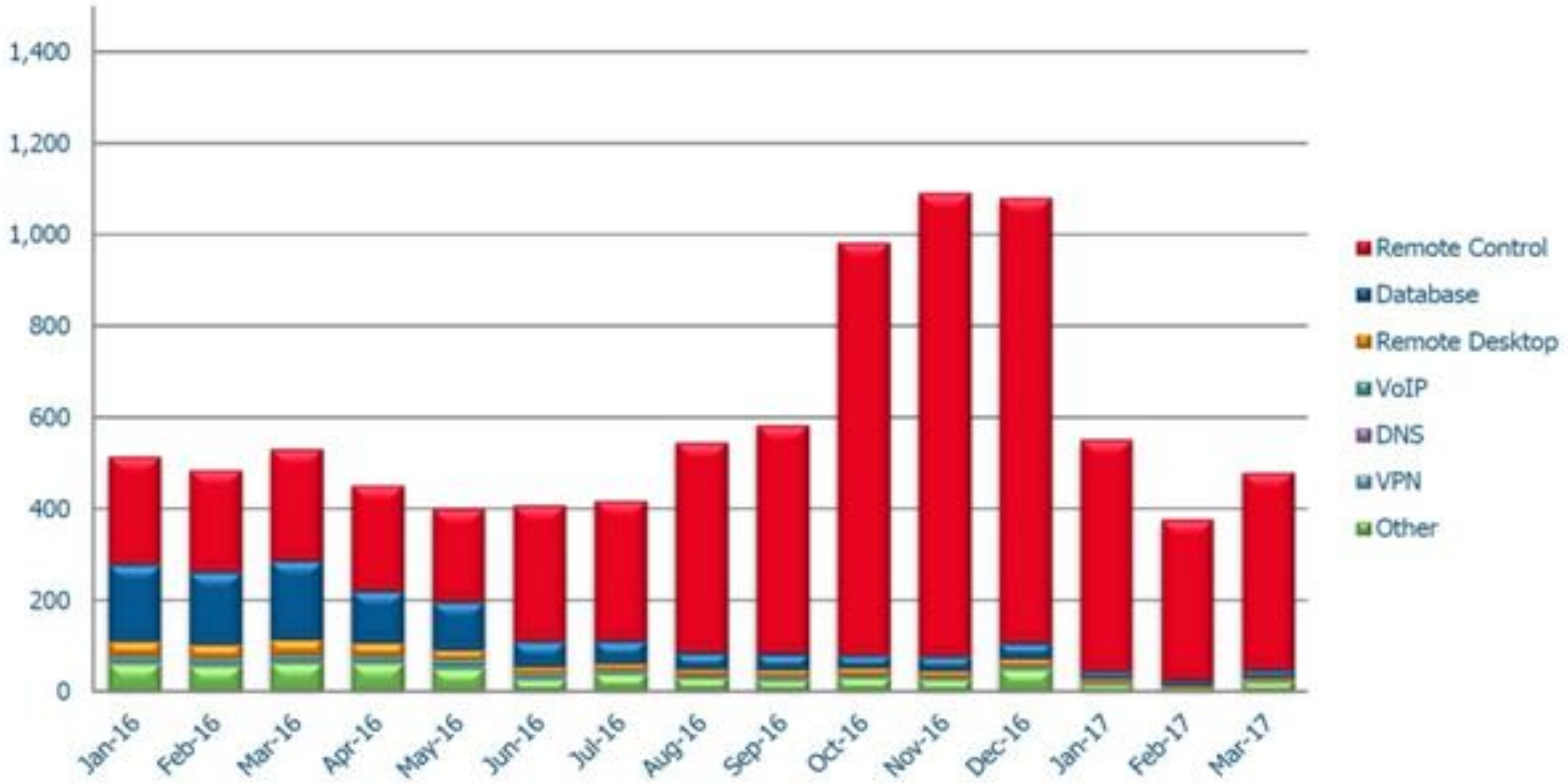
Why cyber security needs to be a topic of boardroom agenda?

- These objectives place two particular demands on organizations: to appoint a suitable official to head up their information security operations, a CISO; and to ensure that the executive and board are appropriately informed of the organization's security status.
- First, the organization has to be very clear on what it wants in terms of the job the CISO is expected to perform and the corresponding attributes that such an incumbent would need to possess.

Why cyber security needs to be a topic of boardroom agenda?

- The CISO is a senior-level executive and rather than being a specialized technical expert, the CISO should be an excellent communicator.
- This will help address the second issue, which is how effectively the CISO can communicate with the board.
- However, organizations need to embrace their concern about cybersecurity and build it into their selection criteria for board members

Cyber attacks per business per day



The average number of attacks per business per day in 2017

Cyber Insurance

- Cyber-insurance is an insurance product used to protect businesses and individual users from Internet-based risks, and more generally from risks relating to information technology infrastructure and activities.
- Risks of this nature are typically excluded from traditional commercial general liability policies or at least are not specifically defined in traditional insurance products.

Cyber Insurance

- Cyber-insurance is a risk management technique via which network user risks are transferred to an insurance company, in return for a fee, i.e., the insurance premium.
- Examples of potential cyber-insurers might include ISP, cloud provider, traditional insurance organizations.

Cyber Insurance

- As of 2014, 90% of the cyber-insurance premium volume was covering exposure in the United States.
- With cyber insurance premiums expected to grow from around $2 billion in 2015 to an estimated $20 billion or more by 2025, insurers and reinsurers are continuing to refine underwriting requirements.
- Market immaturity and lack of standardization are two reasons why underwriting cyber products today make it an interesting place to be in the insurance world.

Cyber Insurance

- Not only do you have an insurance marketplace that's trying to reach a standard and accommodate the needs of today's insured, but you also, at the same time, have a rapidly developing exposure landscape and capacity available.

Types of cyber insurance

- **Hacksurance** - Insurance against cyber attacks and hacking attacks.
- **Theft and fraud.** Covers destruction or loss of the policyholder's data as the result of a criminal or fraudulent cyber event, including theft and transfer of funds.
- **Forensic investigation.** Covers the legal, technical or forensic services necessary to assess whether a cyber attack has occurred, to assess the impact of the attack and to stop an attack.
- **Business interruption.** Covers lost income and related costs where a policyholder is unable to conduct business due to a cyber event or data loss.
- **Extortion.** Provides coverage for the costs associated with the investigation of threats to commit cyber attacks against the policyholder's systems and for payments to extortionists who threaten to obtain and disclose sensitive information.
- **Reputation Insurance** : Insurance against reputation attacks and cyber defamation.
- **Computer data loss and restoration.** Covers physical damage to, or loss of use of, computer-related assets, including the costs of retrieving and restoring data, hardware, software or other information destroyed or damaged as the result of a cyber attack.

Reducing Cyber risk

- The term “cyber risk” refers to a multitude of different sources of risk affecting the information and technology assets of a firm.
- We thus define cyber risk as “operational risks to information and technology assets that have consequences affecting the confidentiality, availability or integrity of information or information systems”

Reducing Cyber risk

- Following the operational risk frameworks in Basel II and Solvency II, we categorize cyber risk into four classes:

1) actions of people (e.g. inadvertent loss of data by employee),

2) systems and technology failures (e.g. malfunction of hardware),

3) failed internal processes (e.g. insufficiently defined responsibilities),

4) external events (e.g. fire)

Reducing Cyber risk

- Schultz et al. 2017 provided a system and method to forecast the risk of targeted cyber-attacks.
- The described technology quantifies linear and non-linear damages to network-dependent assets by propagating probabilistic distributions of events in sequence and time in order to forecast damages over specified periods.
- Damage-forecasts are used to estimate probabilistically time-varying financial losses for cyber-attacks.
- The described technology incorporates quantities and dependencies for pricing insurance, re-insurance, and self-insurance, assessing cost-benefit tradeoffs for sequenced implementation of security control measures, and detecting attacks in the targeted network

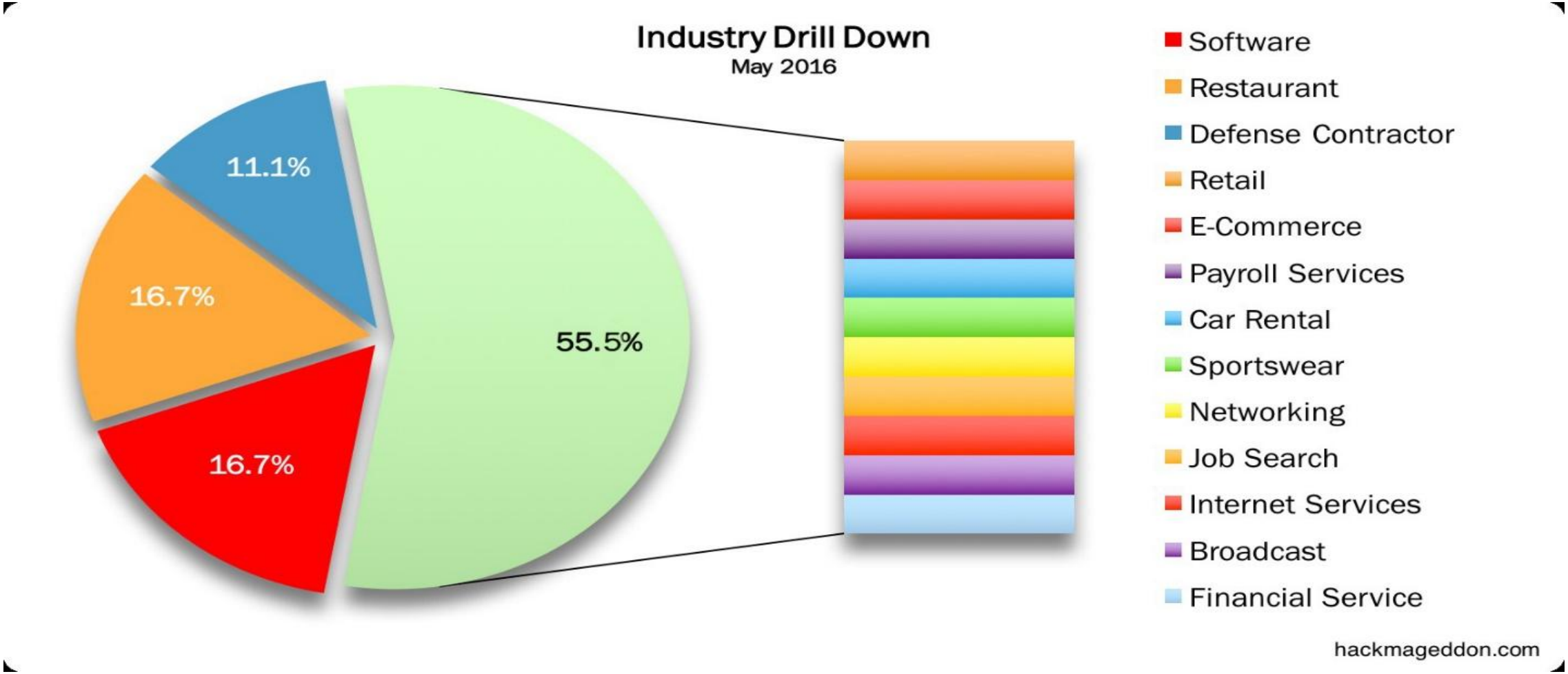
Reducing Cyber risk

- A method for cyber-attack risk assessment is disclosed. Zandani 2018, worked on this method during a study.
- He claimed that the method uses at least one hardware processor for: continuously collecting, from a networked resource, cyber-attack data having multiple attack methods directed at multiple objectives.
- The method also collects organizational profile data, having: assets, each relevant to at least one of the objectives, and defensive controls, each configured to protect at least one of the assets by resisting one or more of the attack methods.
- The method continuously computes: an enterprise risk score, and an asset risk score for each of the assets.
- Each asset risk score is computed with respect to: the attack methods directed at the objectives relevant to the asset, the defensive controls provided to protect the asset, and a maturity score representing the capability of the defensive controls to protect the asset.

Reducing Cyber risk

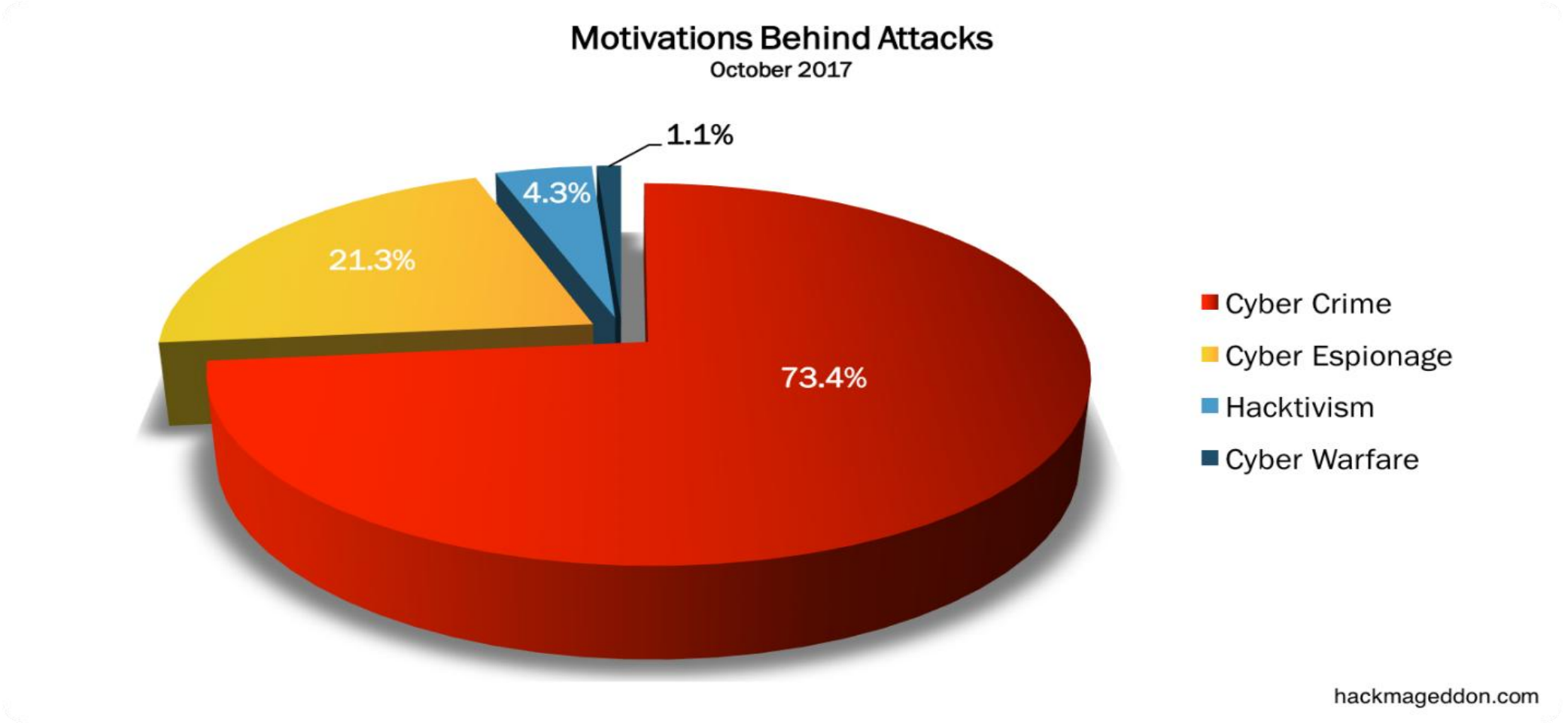
- To avoid cyber threats, we need to properly manage the cyber-risks and the cyber- security.
- Managing cyber security in an organization involves allocating the protection budget across a spectrum of possible options. This requires assessing the benefits and the costs of these options.
- The risk analyses presented here are statistical when relevant data are available, and system-based for high-consequence events that have not happened yet.

The importance of cyber risk in the organization is when we know that many industries are exposed to security threats. The figure below shows the industry drill down in May 2016.



Industry Drill down, May 2016

One of the issues that we deal with in cyber risk in organizations is the attackers' motive for cybercrime. The figure below shows the motivation behind attacks.



Motivation behind attacks

Increasing Cyber Security

- Cyber security has been one of the biggest concerns of organizations over the recent years.
- The days when companies moved cyber security concerns to the IT department because it has become more and more a business issue.
- This is especially important because businesses have become more digitized, meaning that they will be exposed to more threats if they do not manage the security risks properly.
- Businesses can no longer cope with traditional methods of information security and have a coherent security plan.

Increasing Cyber Security

- Technology has made it more difficult to steal automobiles.
- Warning systems are connected to ultra-smart computer systems that can shut down the car, send GPS tracker information to the authorities, and report problems to the owners through smartphones.
- But while computers have been doing a lot of work to secure cars and other objects, it's likely that these computers and networks are more and more at risk.
- The problem seems to be inherently intrinsic: computers protect everything, but who protects them?
- In fact, the enormous amount of computer tools all connected to the networks around us has made the work of information security companies more difficult to protect businesses against the many threats that exist today.
- The same factors have enhanced the issue of cyber security in organizations because it directly interacts with the profitability of organizations.

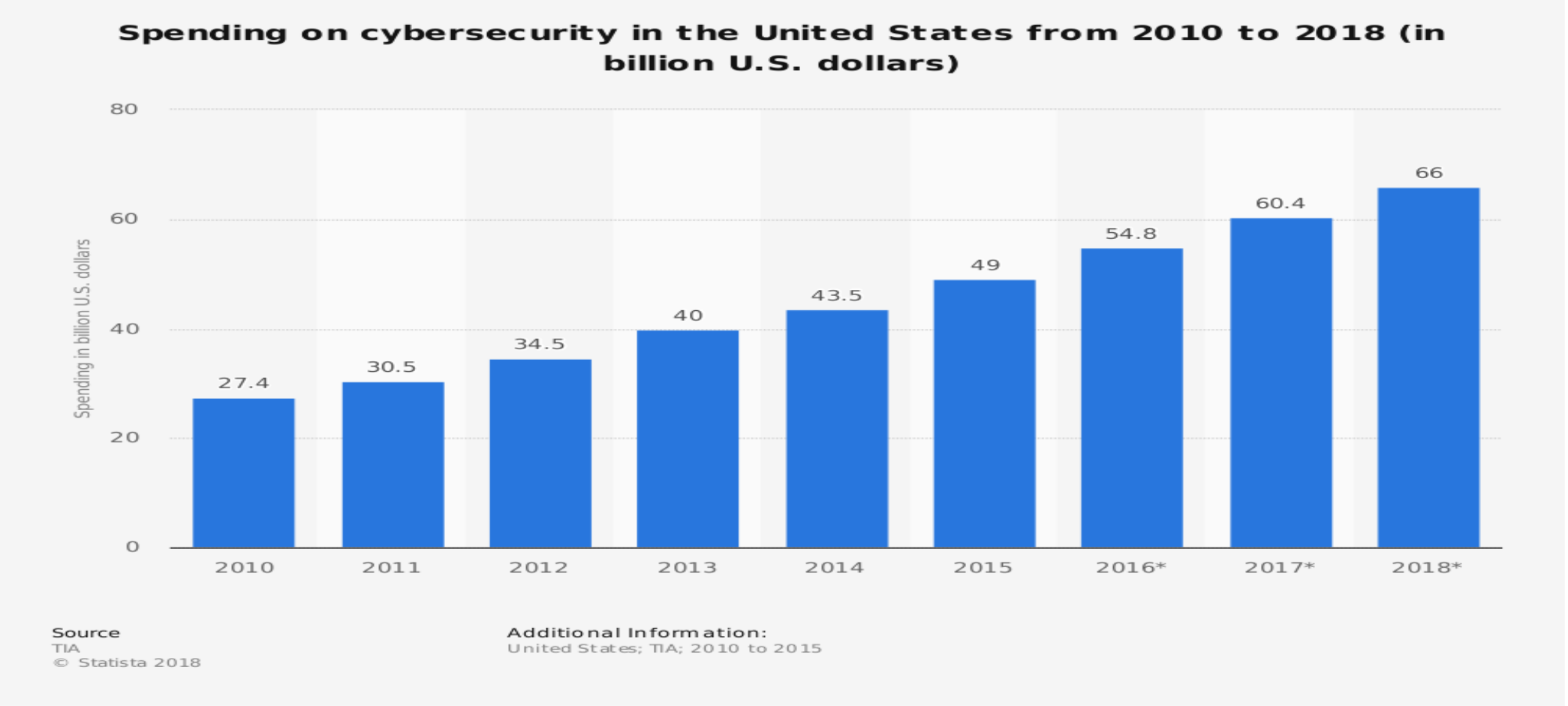
Increasing Cyber Security

- The term cyber security is often used interchangeably with the term information security but it seems that, although there is a substantial overlap between cyber security and information security, these two concepts are not totally analogous.
- Moreover, cyber security goes beyond the boundaries of traditional information security to include not only the protection of information resources, but also that of other assets, including the person him/herself.
- In information security, reference to the human factor usually relates to the role(s) of humans in the security process.
- In cyber security this factor has an additional dimension, namely, the humans as potential targets of cyber-attacks or even unknowingly participating in a cyber-attack

Increasing Cyber Security

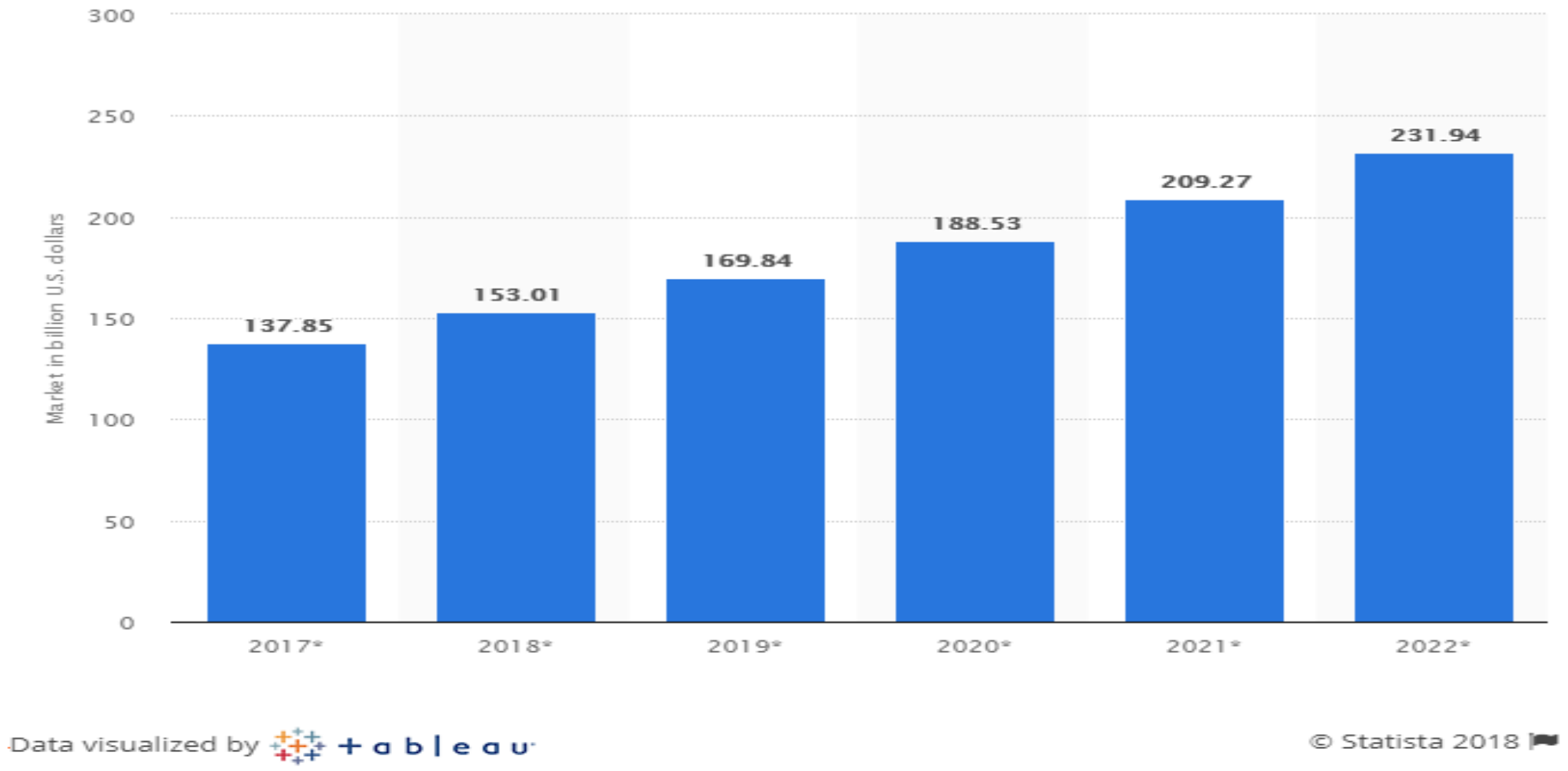
- One of the major issues mentioned is the cost of the attacker, which can be added to the increasing time of attack.
- In the discussion of cyber-attacking, when we increase the time and cost of the attacker, in fact, part of his power is reduced.
- As a result of cyber security arrangements, it responds better. For example, we can call the story of a lock and thief.
- No lock in the world can stop all the thieves, but there is more lock to increase the time and cost of the thief.
- In cyber-security discussions, by increasing the time and cost of the attacker, the organization has raised its cyber security.

The statistic shows the cyber-security spending in the United States from 2010 to 2018.
In 2014, the spending on cyber-security in the United States reached 43.5 billion U.S. dollars.



Spending on cyber-security in the United States from 2010 to 2018 (in billion U.S. dollars)

The statistic depicts the size of the cyber security market worldwide, from 2017 to 2022. In 2017, the global markets that use cyber security, are expected to reach 137.85 billion U.S. dollars.



Size of the cyber security market worldwide, from 2017 to 2022

Business cyber security plan

- Businesses of all sizes can ensure they have the protection they need to keep themselves safe.
- The best way to defend your business against cybercrime is preparation.
- One way you can prepare your business for a cyber-attack is to establish a cyber-security plan.
- A cyber-security plan is a document specific to your business that outlines the proper and safe way to use technology in a business capacity.
- You can tailor it to the needs of your business and employees while still providing protection.

Business cyber security plan

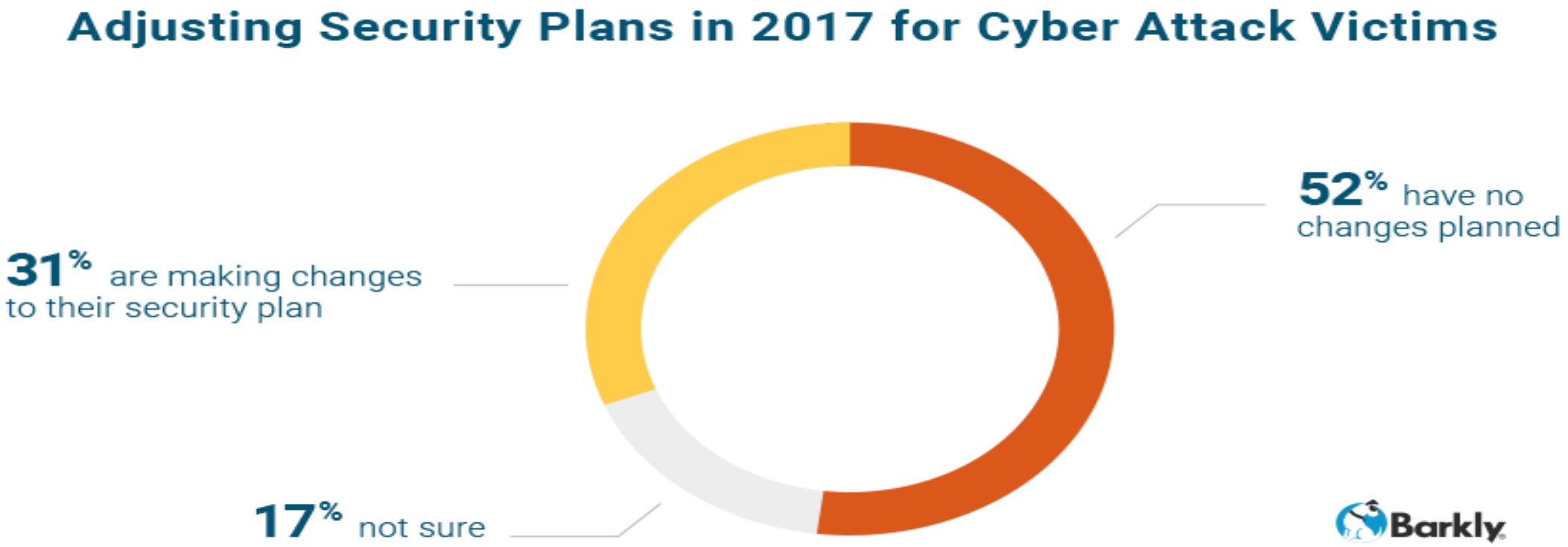
- Terry Benzel 2015, researched about a Strategic Plan for Cyber-security Research and Development.
- In this research, he claimed that, the US government and its international partners are creating the Cyber-security Research and Development Strategic Plan, which will be used to guide government funding for programs, policies, investments, and collaborations for the next five years.

Business cyber security plan

- In 2011, the NITRD published “Trustwor-thy Cyberspace: Strategic Plan for the Federal Cyber-security Research and Development Program,” a coordinated effort involving leading researchers, industry, and government.

- The Cyber-security Enhancement Act of 2014 spurred changes to this strategy, examining the 2011 federal plan and identifying areas in which its priorities should change-for exam-ple, removing some topics, continuing areas previously identified, and adding new areas and challenges

52% of organizations that suffered successful cyber-attacks in 2016 aren't making any changes to their security in 2017 and this is not suited to their future. 31% are making changes to their security plan. As cyber threats are growing, the change in cyber security plan is wiser.



Adjusting security plans in 2017 for cyber-attack victims

Research achievements

1) Given the cyber threats and the critical role that CISO has found today in organizations, the role of cyber security in board meetings has also become more pronounced. Since cyber security is an important part of protecting and increasing the profitability of an organization's business, it seems that discussing cyber security is one of the main needs of the board.

Research achievements

2) Since cyber threats have increased sharply in recent years, especially from 2017 onwards, and these threats have a profound impact on the profitability of organizations, organizations must take measures to address these threats.

Therefore, investing in forecasting and managing cyber-risk should be one of the most important strategic plans for the company.

As cyber threats pervade the profitability of an organization's business, by enhancing cyber security, the organization's profitability can also be sustained.

Also, cyber security measures can save organization time and cost, but increase the attacker's time and cost.

Hence, the organization seems to have taken a major step in securing its profitability by raising its cyber security, which justifies the cost of cyber security.

Research achievements

3) Companies that include cyber insurance in their planning seem to be safer than possible future cyber threats. Although there is no 100% guarantee of cybercrime security, companies with cyber insurance can minimize cybercrime.

So it seems that, with minimal cyber risk, the profitability of the company's business rises and Investment on cyber insurance is justified.

Research achievements

4) When we are aware of the importance of cyber security in the organization and its direct link with the profitability of the organization, we need to close the cyber security plan to the business organization.

Thank you

ITU CENTRES OF EXCELLENCE NETWORK FOR ASIA-PACIFIC REGION
ITU- ICT Faculty training on “Cybersecurity” 12-16 May 2018 - Tehran, Islamic Republic of Iran