# Framing a security message

* + Its not the an after thought
  + Its not because “they” are specifically targeting “us”
  + Its not because crypto apis and firewalls are awesome
  + Its not “stopping hackers” … its about stopping fat finger bob!

It can be difficult to communicate a desired security posture, because the ideas can seem foreign and not directly relevant. How many times, have you heard someone state that they do not need to consider security because I’m not important and not worth their time? If the ideas of security are not applicable then why should there be any investments into the concepts, surely it is more economical to use those resources towards more meaningful activities.

This perception is inaccurate specifically because it uses a legacy view of the role security, where a more modern position needs to consider the overall risks to the business.

# What is the goal of security

* + Prevent *negligence*, erroneous behavior, and maliciousness

The purpose of security is to ensure the individual features and services are able to perform at a consistent level, despite erroneous behavior. This approach to risk needs to consider the influence of both negligence and malicious actions. For instance, when a developer connects to a production database and begins executing sql commands, their goal is most likely to assist a customer, however an incorrectly typed command could corrupt the state. Systems need to be in place for asserting this employee cannot cascade failures.

Later when a customer requests to delete a record that contains a single quote, and this triggers a SQL injection, they are again not being malicious only trying to use the product as it expected. How will the consistency across opaque text be maintained? What if that error causes additional state to become corrupt, does a recovery process exist or is that information permanently lost?

# How has the perception evolved?

* + Focus on individual attackers
  + Focus on technology
  + Focus on national states
  + Focus on assume breach
  + Focus on people

The legacy view of cybersecurity focuses on the idea that an individual malicious attacker is out to get us. Under this perception the organization needs to provision a firewall and similar technology, and that individual is kept out. Problem solved, right?

Unfortunately, this is an oversimplification, the attackers are not an individual but instead collections of mindless automation. These scripts leverage search engines to find vulnerability signatures, and then enumerate different attack scenarios from their botnets. Since, only the most sophisticated hackers or nation states could have enormous botnets, those are the only individuals to keep out?

Unfortunately, this is again oversimplification, the ubiquitous access to cloud computing and high speed networks, allows anyone to create disposable infrastructures that instantly scale to any size and cost pennies per hour. These systems are available for use by both the honest and criminal businesses. Now that there is a mechanism for anyone to run automation and on a large scale, we need to assume that our business on the internet is not special, only a random endpoint for automation to attack.

However, though a game of cat and mouse, technology continues to create more advanced and adaptive filters for our network services. But what about the people? They are the most important asset in the organization and yet we are doing little to protect them. Not only do they hold all the keys to the kingdom, more than willing to give away their access in the spirit of being helpful.

# Why are people now the focal point

* + 50% attacks are technology malicious
  + 25% attacks are malicious against humans
  + 25% attacks are human errors

Despite such attention to ensuring technology is secure, the human scenario is often ignored entirely. According to XXXX, approximately half of the threats to business continuity come from the employees as they interact with malicious automation or make mistakes. An all to common scenario is for the engineering team to deploy new features without considering the performance and scalability, only to have it create a surge of traffic that prevents a dependent traffic from functioning.

So, by making security patterns and practice a precursor to design the threat landscape is reduced by half. For the other half, technology, these are challenges for other technology solutions to address. The human challenges can only be addressed through awareness and training.

# Where do we need to protect humans?

* + Network borders are abstract
  + Connections come across heterogeneous devices
  + Insiders
  + Any communication/interaction could result in undesirable behavior

Before the internet the attack surface was limited to criminals breaking down the front door and stealing the safe. Now businesses are highly connected through always on technologies that interact with the outside world. Critical infrastructure, like DNS and LDAP, also resides outside of the corporate firewall creating a more abstract notion of where the network ends.

Networks need to consider the impact of heterogeneous devices, that are not completely under the control of the administrators. How many iPads and Android phones hold sensitive information but have more than policy governance to ensure desired configurations. Or how many work laptops also surf the public internet, placing them at risk for drive-by exploits.

Though these are not the only mechanisms to interact with the employees, they also receive emails, snail mails, voice calls, and video chats. Each of these mediums invites attack vectors where scammers can attempt to slip unauthenticated messages. If an attacker can send a message on official letterhead, and change a policy why bother with a more complex assault?

# Understanding STRIDE categorizations

* + Spoofing
  + Tampering
  + Repudiation
  + Information Disclosure
  + Denial of Service
  + Elevation of Privileges

1. How do these apply to humans
   * Getting a free cup of coffee
2. How can we define the coffee in terms of threat modeling
   * Assets, endpoints, trust boundaries, protocols, and threats
3. Creating a security aware culture
   * Security is about risk management protections
   * Be skeptical
   * Authenticate, authorize, and audit actions
   * Preventing negligence, how will this fail?
     1. Think about quotas, fail-over, backup/recovery
   * Preventing maliciousness
     1. Think about where data and commands become collide
4. Credential management
   * Influence of password policies
   * Influence of SSO/OAuth
   * Influence of MFA
     1. Something you know
     2. Something you have
     3. Something you are
     4. Somewhere you are
     5. Something you do (gestures)
5. Device Management
   * Software patches
   * Desired Configuration Policies
   * Malware
6. Phishing sites
   * Why do they work
   * Why do these protections fail?
7. Doxing
   * Social networks
   * Publications
   * Public information
   * … resulting in advanced spear phishing
8. Untrusted networking
   * The starbucks attack
   * DNS attacks
   * Discussing work issues outside of work
   * Unencrypted devices
9. Challenges with internationalization
   * GDRP
   * Chinese Cybersecurity Law
   * Notions of sovereignty
10. Conclusions