

# Secureworks®



06 September 2018

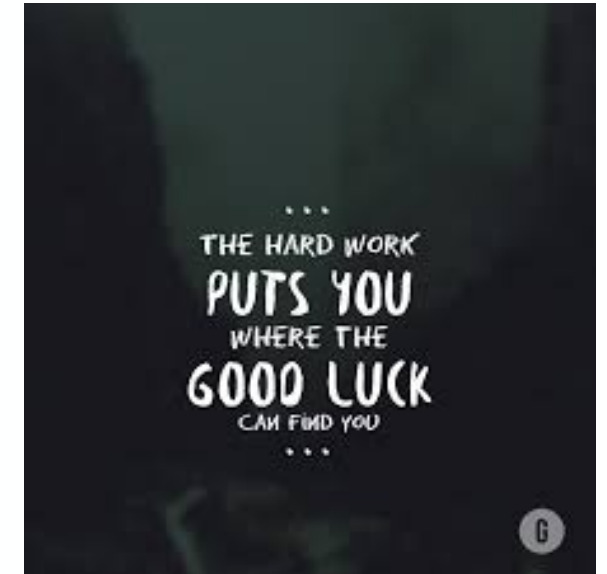


# Partnerships Needed to Meet Today's Security & Privacy Requirements

- **About Me...**
- **Today's Challenges**
  - **Changing Technologies**
  - **Expectations**
- **Compliance ≠ Security**
- **Partnerships**
- **Questions & Contact Information**

# About Me...

- **Managing Principal Consultant, Secureworks**
- **25+ years of experience in cyber security**
- **12+ years of experience in privacy**
- **Previous experience**
  - Chief Privacy Officer & Director, Global IT Governance & Compliance, The Coca-Cola Company
  - Senior Manager, Computer Forensics & Incident Response, pwc
  - Manager & Senior Technical Staff, CERT® (Carnegie Mellon University)
  - User Consultant, PREPnet
  - Buyer, Fashion Retail Industry



# Today's Challenges

## Some of our key challenges...

- **Hacker vs Company (or an individual user)**
- **Changing technologies**
- **Expectations**
  - **Users**
  - **Leaders**
  - **External Stakeholders (e.g., Shareholders)**
  - **Legal**
  - **Consumers**



# Today's Challenges

## Hacker vs Company (or an individual user)

- **Still...**
  - **Hacker needs to find/exploit a single vulnerability**
  - **Company/user must fix/patch/close all vulnerabilities so that the hacker cannot find a single one...**
  - **Ransomware – are you prepared?**
    - **Company**
    - **Individual**





# Today's Challenges

## Changing Technologies

- New Technologies
- New Features in “old” Technologies
- New Development Approaches
- On prem vs cloud
- Enterprise vs Consumer Technologies



# Today's Challenges

## Changing Technologies (cont.)

- **New technologies**
  - “Good old days” →
    - Bought solution that lasted years (sometimes decades)
  - Today
    - Not just upgrades, but new solutions
      - Implement
      - Train
      - Must be flexible & have an architecture to support rapid changes
  - Testing before deployment
  - Deploy to geeks vs executives
  - Do you want to be the 1<sup>st</sup> to implement/use?  
Or wait to be a later adopter?



# Today's Challenges

## Changing Technologies (cont.)

- **New features in “old” technologies**
  - **Same as new technologies**
    - **Except that users often “hate” learning new features**

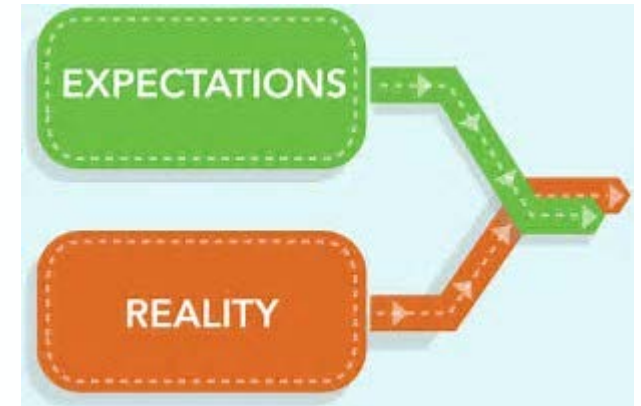




# Today's Challenges

## Changing Technologies (cont.)

- **Expectations**
  - **Users**
    - **Ease of use**
    - **Use consumer technologies/apps/capabilities for enterprise use**
  - **Leaders**
    - **Enable the business without risking intellectual property**
    - **Technologies enable business to move faster**
  - **External Stakeholders (e.g., Shareholders)**
    - **More competitive business**
    - **Protecting intellectual property**
  - **Legal**
    - **Changing laws & regulations**
      - **Security & privacy**



# Today's Challenges

## Changing Technologies (cont.)



- **New development approaches**
  - **Agile vs Waterfall vs DevOps**
    - **Waterfall:** sequential design process. This means that as each of the eight stages (conception, initiation, analysis, design, construction, testing, implementation, and maintenance) are completed, the developers move on to the next step
    - **Agile:** set of principles for software development under which requirements and solutions evolve through the collaborative effort of self-organizing cross-functional teams
    - **DevOps:** software engineering practice that aims at unifying software development (Dev) and software operation (Ops); the main characteristic of the DevOps movement is to strongly advocate automation and monitoring at all steps of software construction, from integration, testing, releasing to deployment and infrastructure management with the aims at shorter development cycles, increased deployment frequency, & more dependable releases, in close alignment with business objectives
  - **“Fail Fast”**

# Today's Challenges

## Changing Technologies (cont.)

- **On prem vs cloud**
  - On prem
  - **SaaS (Software as a Service)**
  - **PaaS (Platform as a Service)**
  - **IaaS (Infrastructure as a Service)**
- **Different**
  - **Oversight/management**
    - **Skills of staff**
    - **Skills of Service Provider**
  - **Legal concerns/requirements**



# Today's Challenges

## Changing Technologies (cont.)

- **Enterprise vs consumer technologies**
- **Developed by a vendor**
  - Tested
  - Supported
- **Developed by consumers but now being used by enterprises**
  - **EULAs vs enterprise license agreement**
    - “anyone” can agree to a EULA; usually authorized signer for enterprise license agreement
  - **Often no support, no further development/enhancements**
    - Just move on to the next consumer app...
  - **Who owns the data?**



Metlin Project 4 - 47406.mproject1

# Today's Challenges

## Expectations

- **Users**
- **Leaders**
- **External Stakeholders (e.g., Shareholders)**
- **Legal**
- **Consumers**





# Today's Challenges

## Expectations (cont.)

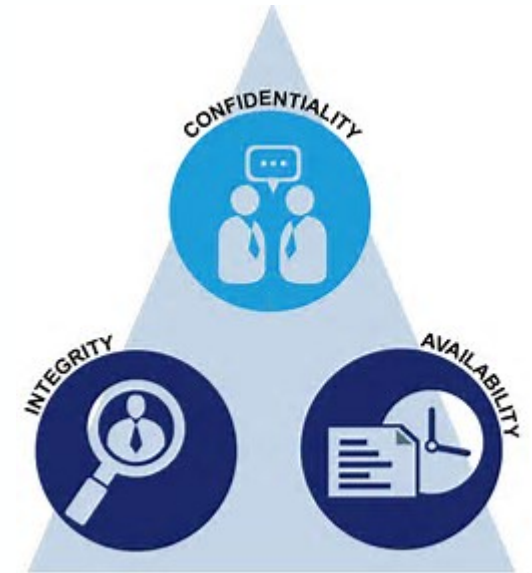
- **Users**
  - **Easier**
  - **Faster**
  - **Use the same technologies at work as at home**
  - **User the same devices at work as at home**
  - **Work from anywhere**
  - **Access data/information anytime/anywhere**



# Today's Challenges

## Expectations (cont.)

- **Leaders**
  - **Users are more productive & efficient through technologies**
  - **Data is CIA**
    - **Confidential (i.e., protected)**
    - **Integrity (i.e., accurate)**
    - **Available (i.e., only to those with business need to access)**



# Today's Challenges

## Expectations (cont.)

- **External Stakeholders (e.g., Shareholders; Customers; Regulators; etc.)**
  - **Similar to leaders**
    - **Company is more productive & efficient**
    - **Data is CIA**



CUSTOMERS



COLLEAGUES



SHAREHOLDERS

# Today's Challenges

## Expectations (cont.)

- Legal
  - Changes in laws & regulations
    - Security & Privacy
  - How to meet security & privacy legal requirements/expectations while enabling the business to move faster



# Today's Challenges

## Expectations (cont.)

- **Consumers**
  - **Companies (& governments) are**
    - **Collecting only the data they need from me**
    - **Collecting my data in a secure/protected manner**
    - **Using my data as was told to me as a consumer**
    - **Not sharing my data with other companies unless I know/agree to it**
    - **Deleting my data when no longer needed**
      - **Securely**
      - **Secure physical disposal**
  - **Companies can anticipate what I may need based on the data that I shared with them...**





# Compliance ≠ Security

## Examples

- **SOX**
  - Enron
- **PCI**
  - TJ Maxx breach (2007)
    - Had been certified by PCI assessment
    - 45.6 million cards compromised
- **Privacy**
  - Target breach (2013 - 2015)
    - 42 million cards compromised
    - 61 million people had PI compromised
  - OPM breach
    - 21.5 million people had PI compromised
  - Equifax
    - 143 million people had PI compromised



# Compliance ≠ Security

## Risk Management

- If compliance ≠ security – then what do we do?
- Most organizations cannot protect all assets equally – and probably should not
  - Too costly
  - Too resource-intensive
- Risk Management
  - Identify sensitive assets
    - IP (Intellectual Property)
    - PI (Personal Information)
  - Insider threat vs external threats
- Need the partnership to make good risk management decisions



# Partnerships

## Partnership is Key...

- **Business, Legal, and IT**
- **Others**
  - **Public Affairs**
  - **Vendors**
  - **Law Enforcement**
- **Must speak in each other's languages**
- **Must understand risk tolerance**
- **Must invest in knowledge/understanding of technologies**
- **Must understand that there will be an incident/breach**
  - **Preparedness**
    - **Effectiveness & Efficiency**
  - **Response time**
    - **Who, What, Where, When, & How...**



# Partnerships

## Roles

- **Business**
  - “Owner” of the data
    - HR, Marketing, Customer, etc.
- **Legal**
  - Provide the legal/regulatory requirements for
    - Business owners of data
    - IT
- **IT**
  - Technology enables organizations to align with privacy laws, regulations, and expectations









# Partnerships

## Roles (cont.)

- **Public Affairs**
  - **Communications**
    - **Internal**
    - **External**
- **Vendors**
  - **That's where the data is...**
- **Law Enforcement**



# Partnerships

## In Closing

- **We need to work together – Business, Legal, IT, Public Affairs, Vendors, Law Enforcement, etc. – to ensure enable the business while protecting company assets**



# Questions & Contact Information

- Katherine Fithen  
Managing Principal Consultant  
Secureworks®  
[kfithen@secureworks.com](mailto:kfithen@secureworks.com)  
+1-770-331-2092



Secureworks®