“Privacy is a fundamental human right ... Privacy underpins human dignity and other key values such as freedom of association and freedom of speech.”

Source: Privacy International, Sept 2015
REALITY is a little messy

• Privacy means different things in different countries.
• Privacy means different things to different generations.
• Privacy requires implementation of security control... controls which may subvert the goals of privacy protection.
Percentage of millennials who would be willing to give away more personal information for a better on-line shopping experience?

1. 56%
2. 23%
3. 7%
Percentage of millennials who would be willing to give away more personal information for a better on-line shopping experience?

1. 56%
2. 23%
3. 7%

Source: Direct Marketing Association
Top 3 Drivers of Privacy Protection (aka Privacy) Regulation World-Wide

- **To promote electronic commerce.** Many countries, especially in Asia, Canada and the U.S., have developed laws in an effort to promote electronic commerce. These countries recognize consumers are uneasy with their personal information being sent worldwide.

- **To ensure laws are consistent with Pan-European laws.** Most countries in Central and Eastern Europe are adopting new laws based on the Council of Europe Convention and the European Union Data Protection Directive.

- **To remedy past injustices.** Many countries, especially in Central Europe, South America and Africa, are adopting laws to remedy privacy violations that occurred under previous authoritarian regimes.

The patchwork of privacy laws

SOURCE: Forrester’s 2014 Data Privacy Heat Map
Practically (my definition)…

**PRIVACY:** The right of an *individual* to

– Control your own personal information,
– Not have it disclosed, used or modified by others without permission.
Privacy protection regulations require:

- **Be accountable** — Establish ownership and accountability within the organization for confidentiality, integrity, and availability
- **Identify & document purposes** — Identify the reasons for obtaining private information from an end user, make those reasons available to the end user
- **Ensure consent** — Establish mechanisms for gaining consent of the end user before collecting private information
- **Limit collection** — Limit collection of private information to only that information you need for business purposes
- **Limit use, disclosure and retention** — Limit use, disclosure only for the purposes for which you have gained consent. Limit retention of information to a time period specified by law and/or consent
- **Ensure accuracy** — Ensure that information collected is accurate
- **Implement safeguards** — Implement administrative, technical, and physical controls around information in order to ensure its confidentiality, integrity, and availability
- **Create openness** — Create a culture of openness, so that if the confidentiality, integrity or availability of the information is breached in a significant way that the end user is notified
- **Provide recourse** — Provide the end user with documented escalation policy and process.
SECURITY is the means used to protect the confidentiality, availability and integrity of personal information through physical, technical and administrative safeguards.
COMMERCIAL BREAK: Privacy Protection is only one of 4 risk domains involving/leveraging Security

<table>
<thead>
<tr>
<th>The BIG Four</th>
<th>Cyber War/Unrest (Emerging Focus)</th>
<th>Cyber Espionage (Emerging Focus)</th>
<th>Cyber Crime (Existing Focus)</th>
<th>Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Requirement:</td>
<td>▪ Assure the availability and integrity of critical infrastructure assets for the purpose of ensuring the public good</td>
<td>▪ Assure the confidentiality, integrity, and availability of select data sets considered “crown jewel” by the organization.</td>
<td>▪ In order to mitigate the risk of money laundering, fraud the general requirement is to protect integrity, availability and authenticity of financial transactions</td>
<td>▪ Assure the confidentiality, integrity, and availability of personally identifiable information in order to protect fundamental human rights</td>
</tr>
<tr>
<td>Buzzwords:</td>
<td>▪ Cyber Warfare ▪ Hacktivism</td>
<td>▪ Cyber Espionage</td>
<td>▪ Money Laundering ▪ Fraud ▪ Identity Theft</td>
<td>▪ Privacy ▪ Identity Theft</td>
</tr>
<tr>
<td>Concern owner:</td>
<td>▪ IT Security ▪ CISO ▪ Legal Officer</td>
<td></td>
<td>▪ Financial Crime Unit</td>
<td>▪ Chief Privacy Officer</td>
</tr>
</tbody>
</table>

WHY? Operational Resilience Business Competitiveness Consumer Protection Civil Liberty
Practically, what do businesses worry about (risk)?

Source: Hackmaggedon Index 2014
Security reality – we have all been compromised

1,764,121
Represents the number of security events the average organization of 15K employees will capture weekly

324
of these events represent actual attacks, per week

2.1
of these attacks will result in an incident, per week, – a 22% annual increase

General Keith Alexander, Head of U.S. Cyber Command, in a speech to the American Enterprise Institute

only 1 out of 100
security compromises are ever detected

2014 IBM Cybersecurity Intelligence Index
Over 75% of incidents were associated with the same five industries,

Finance and insurance
Manufacturing
Information and communication
Retail and wholesale
Health and social services

Finance and insurance companies tend to offer attackers the most significant potential payoff.

Source: IBM Security Services 2014 CyberSecurity Intelligence Index
From a practitioner’s perspective, most security incidents are of the “Oops” variety

- Inadvertent Actor (“Oops”)
- Deliberate Actor (Malicious Intent)

Top 3 “Malicious” Incident Types
- Malware Infection
- Access Misuse
- Web-Site Compromise

~1% of all malicious attack result are “noteworthy” (possibly material/significant)

Top 3 “Oops” Incident Types
- Misdirected e-mail
- Lost Laptop
- Stolen laptop
While threat actors are acting “maliciously”, insiders are an “unwitting” accomplice in 95% of incidents.

Source: IBM Security Services 2014 CyberSecurity Intelligence Index

“…over 95% of all incidents investigated recognize “human error” as a contributing factor.”
Top 5 reasons **WHY** compromise was possible

<table>
<thead>
<tr>
<th>End users</th>
<th>Systems Admins/Developers</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Double-clicking “on anything”, plugging “anything” (like a USB) in</td>
<td>1. Connecting systems and virtual images to the Internet before hardening them</td>
</tr>
<tr>
<td>2. Disabling security settings and/or anti-virus when it gets in the way</td>
<td>2. Failing to remove default accounts or passwords, failing to remove old/unused user accounts</td>
</tr>
<tr>
<td>3. Using vulnerable, legacy software and hardware</td>
<td>3. Failing to update or patch systems/applications on a timely basis.</td>
</tr>
<tr>
<td>4. Failing to install security patches (“Remind me Tomorrow”)</td>
<td>4. Using legacy or end-of-life software and hardware</td>
</tr>
<tr>
<td>5. Using a weak or default passwords, or using business passwords for personal use</td>
<td>5. Using insecure remote management software</td>
</tr>
</tbody>
</table>
Why is it crime so easy? IT’S BIG BUSINESS.

Data is bought and sold in “carding forums”
# Attacks-as-service pricing models

<table>
<thead>
<tr>
<th>Cost</th>
<th>Service Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$350-$400 an hour</td>
<td>• Hacker consulting services</td>
</tr>
<tr>
<td>$100 per 1K installs</td>
<td>• Malware infection/spreading services</td>
</tr>
<tr>
<td>$535 for 5 hours a day for one week</td>
<td>• Distributed Denial of Service (DDoS) attack, money back guarantee</td>
</tr>
<tr>
<td>$40 / 20K emails</td>
<td>• Email spam</td>
</tr>
<tr>
<td>$2/30 posts</td>
<td>• Blog spam</td>
</tr>
<tr>
<td>$80 for 20K spammed backlinks</td>
<td>• Blackhat Search Engine Optimization (SEO)</td>
</tr>
<tr>
<td>$500 to $10K</td>
<td>• Crimeware, with premium support levels available</td>
</tr>
<tr>
<td>$150 and $400</td>
<td>• crack e-mail passwords in less than 48 hours</td>
</tr>
</tbody>
</table>
What keeps me up at night….

“In the developing country context in particular, sub-cultures of young men engaged in computer-related financial fraud have emerged, many of whom begin involvement in cybercrime in their late teenage years…”

Source: UNODC 2013

- By 2011, ~33% of the world’s population had access to the Internet.
- By 2017, that percentage will increase to +70%
- 45% of all Internet users are currently below the age of 25 years.

### Cyber juveniles

<table>
<thead>
<tr>
<th>Activity</th>
<th>Secondary school pupils</th>
<th>University students</th>
<th>Marginalised youth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacking</td>
<td>10.3</td>
<td>13.9</td>
<td>24.8</td>
</tr>
<tr>
<td>Stealing gaming coins and/or virtual currencies</td>
<td>17.8</td>
<td>21.9</td>
<td>36</td>
</tr>
<tr>
<td>Triad-related activities</td>
<td>12.4</td>
<td>13</td>
<td>36</td>
</tr>
<tr>
<td>Trafficking drugs</td>
<td>9.1</td>
<td>11.4</td>
<td>19.8</td>
</tr>
</tbody>
</table>

Source: Federation of Youth Group

SCMP
Recommendations
My big five focus areas

1. Train, test, trick employees
   (your weak link)

2. Re-organize security to enable DevOps
   (you can’t escape)

3. Adopt cloud, mobile, social
   (enable radical innovation)

4. Mind the supply chain
   (the other weak link)

5. Invest in next gen threat detection
   (people, process & tech.)
Restructure to support the Agile/DevOps transformation

**STRATEGIC PLANNING SERVICES**
Define security strategy & objectives. Analyze metrics and measure effectiveness of controls. Drive continuous improvement.

**POLICY & ARCHITECTURE SERVICES**
Define the essential security policies, standards and architectures (based on 80/20 rule) which are easy to digest and consume.

**COACHING & ADVISORY SERVICES**
Staff domains with security subject matter expertise required to innovate with confidence. Increase security awareness through educational programs for employees and contractors.

**SECURITY OPERATIONS**
Provide core security monitoring, assessment & response services: Hunter Services, Threat Monitoring Services, and Incident Response.
The emerging SOC (detection & response model)

Technology Platform

Area of radical innovation!
Advanced threat detection via Machine Learning

- **Machine learning** is a process used to train computers to distinguish between classes of objects, and then to predict the class of an object they have never seen before using classifiers.

- Successfully applied in facial recognition, voice recognition, image processing, and medical diagnostics, it is being applied to cyber threat detection by enabling software classifiers to distinguish malware from benign software.

- Machine Learning has distinct advantages over traditional signature and sandbox-based approaches:
  - Scales to very high volumes of traffic,
  - Resilient to evolving malware and tactics,
  - Higher threat detection rates
  - Limited risk of privacy violation
Privacy and security can co-exist, albeit uncomfortably.

As broader cybersecurity regulation in EU and US is introduced, and impact of the Safe Harbor ruling is fully realized, the pendulum will swing from crisis driven security spending to compliance spending.

Capabilities like Machine Learning will address trickier issues associated with security monitoring and analysis.

Investments in DevOps (building security inside) is the only way to systemically “fix” our issues.
Thank you.
There are two reasons why organizations spend money on security

Crisis
(a CXO and/or Board Member read a scary news report)

Compliance
(where I think the pendulum is swinging)
The Pragmatic Approach to Security Risk Management

- As a “theory” started gaining momentum in the late 1990s.
- Focuses on finding a balance between effective security and cost.
- Belied by a fairly simple “Risk Equation”.
- Most regulations/security best practice guides recognize this.

The Axiom… Never spend $100 dollars on a fence to protect a $10 horse.
Security risk exists when ...

Security Risk Management is the application of control...
- to detect and block the threat,
- to detect and fix a vulnerability,
- or to address the impact when all else fails.
How pragmatic security risk management works

PROTECT
Implement and operate control - policy, technology, etc...

IDENTIFY
Define risk map, risk posture, control strategy

RESPOND
Respond and manage security incidents compliance

DETECT
Monitor and analyze security events, 24x7

SecOps
**BEWARE: Security Risk Management in REAL LIFE**

<table>
<thead>
<tr>
<th>Phase</th>
<th>People</th>
<th>Data</th>
<th>Apps</th>
<th>Endpoint</th>
<th>Server</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Identify</td>
<td>Policies, Education &amp; Awareness, Role Management</td>
<td>Policies, Data Classification (Manual)</td>
<td>Asset Management (CMDB)</td>
<td>Mobile Device Management/Asset Management</td>
<td>Asset Management CMDB</td>
<td>Asset Management CMDB</td>
</tr>
<tr>
<td>2. Protect</td>
<td>Identity &amp; Access Mgmt, Biometrics</td>
<td>Encryption, Digital Rights Mgmt</td>
<td>Web App FW, Web &amp; Email Filtering, Access Control, Maintenance</td>
<td>AV, ADS, PFW, IPS, Configuration Mgmt. and Enforcement (MDM on Mobile), Maintenance</td>
<td>AV, IPS, Configuration Mgmt. and Enforcement, Access Control, Maintenance</td>
<td>FW, IDS/IPS Configuration Mgmt. and Enforcement, Access Control, Maintenance</td>
</tr>
<tr>
<td>4. Respond</td>
<td>Varies</td>
<td>Data Privacy Team</td>
<td>Fraud/AML Team</td>
<td>Emergency Response Team</td>
<td>Emergency Response Team</td>
<td>Emergency Response Team</td>
</tr>
<tr>
<td>5 Recover</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Areas of CONFLICT*
Cyber Crime impact to the individual?

<table>
<thead>
<tr>
<th>Lost/Stolen PII</th>
<th>Identity Fraud (Existing Account Fraud)</th>
<th>Identity Theft (New Account Fraud)</th>
</tr>
</thead>
<tbody>
<tr>
<td>13% Breach victims became a victim of fraud in 2014*</td>
<td>4.64% Incidence Rate*</td>
<td>.29% Incidence Rate*</td>
</tr>
<tr>
<td>85,611,528 Records exposed through breaches**</td>
<td>$14 Billion Annual Losses*</td>
<td>$2 Billion Annual Losses*</td>
</tr>
<tr>
<td>7 Mean Resolution Hours*</td>
<td>25 Mean Resolution Hours*</td>
<td></td>
</tr>
</tbody>
</table>

Source: Javelin Identity Theft Statistics, 2015
Consumers don’t always express concerns in **practical** terms.

**14%**

Of adults surveyed say they have experienced negative consequences due to online activities by others.

Those 14% reported a variety of negative consequences:

- **21%** were fired from a job
- **16%** lost out on getting a job
- **16%** lost their health insurance
- **14%** lost out on the college they wanted
- **15%** were turned down for a mortgage

**56%**

Of adults surveyed don’t actively think about the consequences of their online activities.

**SOURCE:** Microsoft Trustworthy Computing, Data Privacy Day Infograph