Cybersecurity and YOU!!

CYBER RESILIENCE - PREPARE FOR WHEN, NOT IF

James Boyles
Cybersecurity Architect

October 2018
What is cyber resilience?

Cyber resilience is an organization’s ability to continue delivering the intended outcomes despite adverse cyber incidents.

IBM Cyber Resilience
= Security + Resiliency + Network solutions
Why is cyber resilience needed?

Cyber attacks are evolving and on the rise.

Top 5 causes of cyber disruptions

- **61%** Phishing and social engineering
- **45%** Malware
- **37%** Spear-phishing attack
- **24%** Denial of service
- **21%** Out-of-date software

Many organizations are unprepared

- **68%** Lack the ability to remain resilient in the wake of a cyber attack
- **66%** Suffer from insufficient planning and preparedness
- **75%** Have ad-hoc, non-existent, or inconsistent cyber security incident response plans
- **191 days** Average amount of time hackers spend inside IT environments before discovery

Sources:
- Ponemon Institute 2017 Cost of Data Breach Study: Impact of Business Continuity Management
- IBM/Forbes Insights survey of 153 executives at large enterprises worldwide, 2017
World Economic Forum
2018 Global Risks
Perception Survey:

Cyberattacks ranked #3

“Attacks against businesses have almost doubled in five years, and incidents that would once have been considered extraordinary are becoming more and more commonplace.”

Source: World Economic Forum, 2018
Attacks are becoming more costly and more likely

- Average total cost of a data breach in 2017: $3.62 million
- Cost impact for one company impacted by NotPetya: $310+ million
- Estimated global cost of WannaCry attack: $8 billion
- Odds of experiencing a data breach over next two years: 1 in 4

Source:
Often these attacks disrupt business operations instead of garnering financial gain.
Cyber resilience programs are under pressure

**Velocity**
**DIGITAL TRANSFORMATION**

The speed at which organizations evolve must increase
- With the acceleration of cloud SaaS, new asset adoption is rapid
- Business initiatives, such as digital transformation, are moving at an unprecedented pace
- Traditional approaches to threat management can’t keep up

**Complexity**
**ADVANCED THREATS**

The threat landscape is evolving daily, complexity is on the rise
- The asset landscape is changing rapidly, including Cloud, SaaS, BYOD, and IoT
- Advanced threats leverage new attack vectors, motivations, and stealth
- Traditional threat management struggles to comprehensively address this new level of complexity

**Liability**
**NEW RESPONSIBILITIES**

An organization’s obligations are in the spotlight
- Businesses are under heavy public scrutiny to protect data
- Growing regulatory emphasis on security and data privacy, combined with fines, and impact to brand reputation have raised the stakes for all organizations
- Traditional threat management lacks the visibility and responsiveness to contain these risks
Organizations are already overwhelmed

**Data Overload**

Analysts are only able to keep up with about 8% of the information needed to do their jobs.

**Unaddressed Threats**

93% of SOC managers are not able to triage all potential threats. 43% of security professionals ignore a ‘significant number of alerts’.

**Cyber Skills Shortage**

1.8 million jobs unfulfilled by 2022.

"My workload is overwhelming and repetitive."

"I don’t know where to focus my time for the quickest response."

"There is so much information out there, it’s impossible to find what’s useful."
Challenges we hear from CISOs in Federal Government Agencies

- Lack of sufficient skills and administration
- Meet the demands of digital transformation
- Ensure data privacy and compliance
- Mitigate insider threats
- Improve real-time visibility and continuous monitoring
Challenges we hear from CISOs in State and Local Government Agencies

- Deal with aging infrastructures
- Address insufficient IT administration
- Meet the demands of digital transformation
- Ensure data privacy and compliance
- Respond to talent and funding shortage
...and operations teams have a challenging mission

Process intelligence and outthink cyber criminals

Protect critical data, users applications and infrastructure

Respond and recover from incidents quickly
Pain points evolve as cyber attacks increase and change

- Need a more precise, immediate response to a cyber event
- Eliminate extended business interruptions from more frequent attacks
- Retain clean IT and critical business process components to quickly resume company operations
- Demonstrable evidence of capability for audit and compliance
Important questions to build a defense

“Your IT infrastructure or email was wiped out around the world in a matter of hours?”

Key consideration
Protection against large scale, volume attacks

“Are your networks outdated, reliant on hardware based network appliances with minimal network segmentation?”

Key consideration
Help maintain business continuity to become cyber resilient

“How long could you sustain operations if forced to revert to manual operations?”

Key consideration
Know and bolster your security posture
Cyber Resilience

**Cyber resilience** is the ability of an organization to continue to function with the least amount of disruption in the face of cyberattacks. It is an end to end approach that brings together three critical areas: information security, business continuity and network resilience of enterprises to ensure organizations continue to function during cyberattacks and cyber outages.

**Cyber Security**

Cyber security is designed to protect systems, networks and data from cyber crimes. Effective cyber security reduces the risk of a cyberattack and protects organizations from the deliberate exploitation of its assets.

**Business Continuity**

Business continuity provides the capability to resume operations when an event causes a service disruption. Plans for Business continuity address natural catastrophe, accidents and deliberate physical attacks; but now, they must also support resumption of operations following cyberattack disruptions.
Cyber resilience serves a number of IT and risk management disciplines.
Cyber Resilience is a business priority that supports "continuous availability" that allows companies to meet their business outcome objectives.
Let’s focus on the most critical security use cases

Outcome-driven security

Prove Compliance

Stop Threats

Grow Business

- Get Ahead of Compliance
- Enhance Security Hygiene
- Govern Users and Identities
- Detect & Stop Advanced Threats
- Orchestrate Incident Response
- Master Threat Hunting

- Secure Hybrid Cloud
- Protect Critical Assets
- Prevent Advanced Fraud
Our unique approach will help transform your security

Build a security immune system

Deploy meaningful innovations
AI and Orchestration
Cloud Security
Collaboration

Get help from the experts
Industry Consultants
Research & Development
World Class Designers
Build an integrated security immune system

**DATA**
- Data protection
- Data access control

**IDENTITY & ACCESS**
- Privileged user management
- Identity governance and administration
- Access management
- IDaaS
- Mainframe security

**ADVANCED FRAUD**
- Fraud protection
- Criminal detection

**MOBILE**
- Transaction protection
- Device management
- Content security

**APPLICATIONS (APPS)**
- Application scanning
- Application security management

**ENDPOINT**
- Endpoint detection and response
- Endpoint patching and management
- Malware protection

**NETWORK**
- Firewalls and intrusion prevention
- Network forensics and threat management
- Network visibility and segmentation

**THREAT INTELLIGENCE (THREAT INTEL)**
- Threat sharing
- IoCs

**SECURITY ORCHESTRATION & ANALYTICS**
- Security analytics
- Vulnerability management
- Threat and anomaly detection
- Threat hunting and investigation
- User behavior analytics
- Incident response

**RELATED SOLUTIONS**
- Application security management
- Application scanning
- Vulnerability management
- Malware protection
- Endpoint detection and response
- Endpoint patching and management
- Malware protection
- Threat sharing
- IoCs

**PLATFORM FEATURES**
- Criminal detection
- Fraud protection
- Application security management
- Malware protection
- Endpoint detection and response
- Endpoint patching and management
- Security analytics
- Vulnerability management
- Incident response
- Threat sharing
- IoCs
Deploy meaningful innovations

AI and Orchestration  Cloud Security  Collaboration
The future of security is **AI and Orchestration**

What if you could augment your teams’ intelligence and response?

Use AI to gain a head start

Automatically investigate incidents and anomalies to identify the most likely threats

- Quickly gather insights from millions of external sources
- Apply cognitive reasoning to build relationships

IBM QRadar Advisor with Watson

Respond quickly with confidence

Orchestrate a complete and dynamic response, enabling faster, more intelligent remediation

- Create dynamic playbooks built on NIST / CERT / SANS
- Deploy response procedures and expertise

IBM Resilient
The future of security is **Cloud**

Can you confidently say yes to digital transformation?

- **Protection Data**
  - IBM Multi-Cloud Data Encryption

- **Gain Visibility**
  - IBM QRadar Cloud Security Analytics

- **Manage Access**
  - IBM Cloud Identity Connect

---

**Get Help from Experts**

| IBM X-Force Cloud Security Service | © 2018 IBM Corporation |
The future of security is Collaboration
Are you part of the bigger picture?

Join an ecosystem of defenses
Customize your security with 140+ apps on the IBM Security App Exchange

Share real-time threat intelligence
Interact with 41K+ users and 800+ TB of threat intelligence on the IBM X-Force Exchange
Supported by hundreds of open integrations
“We need to secure the records of 475,000+ members while managing critical database access across our hybrid environment... we need help.”
Secure hybrid cloud

- Protect data: IBM Multi-Cloud Data Encryption
- Gain visibility: IBM QRadar Cloud Discovery App
- Manage access: IBM Cloud Identity Connect

Cloud providers: Box, Concur, Google, Office 365, Salesforce, Workday, AWS, Microsoft Azure, VMware, IBM Bluemix.
Secure hybrid cloud

IBM Security Guardium

Secure applications built in a multi-cloud environment

- Automatically discover and classify sensitive data
- Understand data access, spot anomalies, stop data loss
Secure hybrid cloud

IBM Cloud Identity Verify

- Simple strong authentication from the cloud
- Check-box risk assessment and user authentication policies

IBM Verify

Sign in securely from anywhere

Face ID
Big Blue Bank uses your Face ID to verify your identity and keep your account safe.

You have a pending sign-in
BigBlueBank Confirmation #416ba96f
Verify with Touch ID

You have a pending transaction for $1200
Big Blue Bank Confirmation #da465b9d
Verify with Face ID

iOS
Android
IBM Security Guardium

Protect critical assets

Shield the business from data risk with automated compliance and audit capabilities

• Automatically discover and classify sensitive data
• Understand data access, spot anomalies, stop data loss
Protect critical assets

- Identify specific, high-value, business-sensitive information assets
- Gain early visibility into potential risks to data and processes
- Inform executives with a business-consumable data risk control center

IBM Data Risk Manager

Uncover, analyze and visualize data-related business risks
Simplify the management and security of smartphones, tablets, laptops, wearables and IoT

- Cognitive insights to identify policy and app improvements
- Proactively address new vulnerabilities

IBM MaaS360 with Watson

Protect critical assets
Discover identity, build trust

IBM Trusteer

Helps organizations seamlessly establish identity trust across the omnichannel customer journey

- Intelligence service layered with advanced AI and machine learning capabilities
- Scalable and agile cloud platform providing real-time assessments
- Continuous digital identity assurance
IBM Hybrid Cloud Security Services

Grow business with IBM Security Services

- **Real-time visibility across multi-cloud environments**, enforcing security policy across shadow and IT-sanctioned workloads
- **One centralized and simplified view** to manage and monitor security operations
- **Prioritizes roadmap actions** needed to protect workloads
- **Implements an integrated threat management program** to detect, prevent and respond to malicious activity

Scalable Cloud

Value

Visibility
THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2017. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM’s current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.