Securing Journey to the Cloud: Part 2

—

Andrew Lemke
Executive Advisor, Inventor

IBM **Security**

IBM

“A hacker invaded 2 CBS reporters' lives without writing a single line of code”

Interns and Social Media: A Goldmine for Hackers
May 28, 2019 | By Stephanie Carruthers

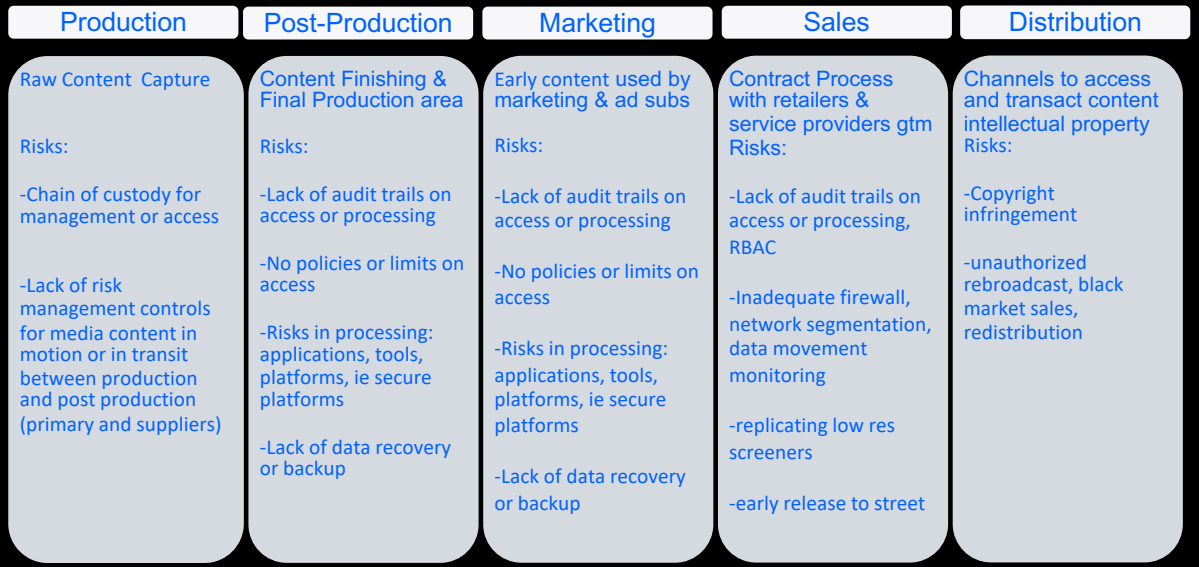
I’m a hacker, and here’s how your social media posts help me break into your company
Stephanie “Snow” Carruthers, the chief people hacker at IBM X-Force Red, shows exactly how easily your innocent shares can give hackers the keys to your company’s kingdom of data.
FastCompany
07.10.2019

Stephanie Carruthers, IBM
Global Social Engineering Expert, X-Force Red
Stephanie leads the social engineering practice, focusing on open-source intelligence gathering, phishing, vishing and physical security assessments for X-Force Red clients.

https://www.youtube.com/watch?v=uhP7NoBJDKU

CBS New June 2019

Media and Entertainment Key Risk Domains



"Content Protection & Security (CPS) Certification Program overview," Content Delivery and Security Association, January 2016, https://www.mesalliance.org/wp-content/uploads/2016/04/ CDSA-Content-Protection-Security-Standard-Overview.pdf.

IBM monitors over 20 APT groups that have compromised companies in the following areas:

- Entertainment & Games software
- Diversified Entertainment
- Information Collection & Delivery
- Internet Publishing, Broadcasting & Search
- Magazine Publishers
- Multimedia, Graphics & Publishing software
- Newspaper Publishers
- TV Station groups

High Risk M&E Cyber Threats Primarily from the following threat actors:

Cybercriminal business operations profiting through targeting the entertainment & gaming industry by stealing account credentials, activation codes, in-game valuables, credit card data, and personally identifiable information. Very similar to enterprise attack styles and TTP's…

Hacktivists groups (in some cases a front for a nation state) seeking to disrupt a target company's business operations to communicate a cause, impact reporting, or manipulate the dissemination of content they view as politically sensitive, controversial, or diametrically opposed to their own views.

APT groups working as subcontractors to their host government in controlling its national image by stealing information related to media organizations reporting activities, including doxing personnel, sources, local partnerships, anticipated public releases, general country governance activities, and specific areas of research.

APT groups engaging in espionage, stealing data related to other companies' mergers, acquisitions, or distribution plans; technologies or processes for advanced production; and creative intellectual property. Overall intent to sell to other regional media and entertainment firms willing to pay for competitive information and advantage.

And as we saw previously, Social Engineering, phishing,….

Industry Threat Analysis

Top Malware Families: the threat intelligence industry most frequently detected threat actors using the following targeted malware families to compromise organizations in the entertainment and media sectors →

- ChinaCopper 59%
- Kaba 15%
- Gh0stRAT 10%
- PoisonIvy 8%
- Page 8%

Top Crimeware Families: the threat intelligence industry shared threat data indicate that the following crimeware variants were the most commonly detected in the entertainment and media sectors →

- Upatre 35%
- Delf 32%
- ZeroAccess 15%
- Allaple 10%
- Muxif 10%

Automation tools

DATA STOLEN FROM ENTERTAINMENT & MEDIA COMPANIES

- Address Books
- Calendar Files
- Executive Communications
- Negotiations Information
- Network Infrastructure Documents
- PR and Marketing Materials
- Reporters' Communications
- User Credentials

CONTENT STOLEN FROM ENTERTAINMENT & MEDIA COMPANIES

- Feature film: audio, subtitles, advertising images, scripts
- Television: audio, close captioning, photos, scripts
- Outtakes: Commentaries, subtitles, infographics, metadata
- Vignettes
- Music video content
- …and more

A successful journey needs security at every phase

Establish
Strategy and Roadmap

Organization-wide Culture Transformation

- Business and technical teams engaged
- Organizational alignment to common goals

Hybrid Multicloud Security Strategy

Define future state, shared responsibility model , build transformation strategy and roadmap

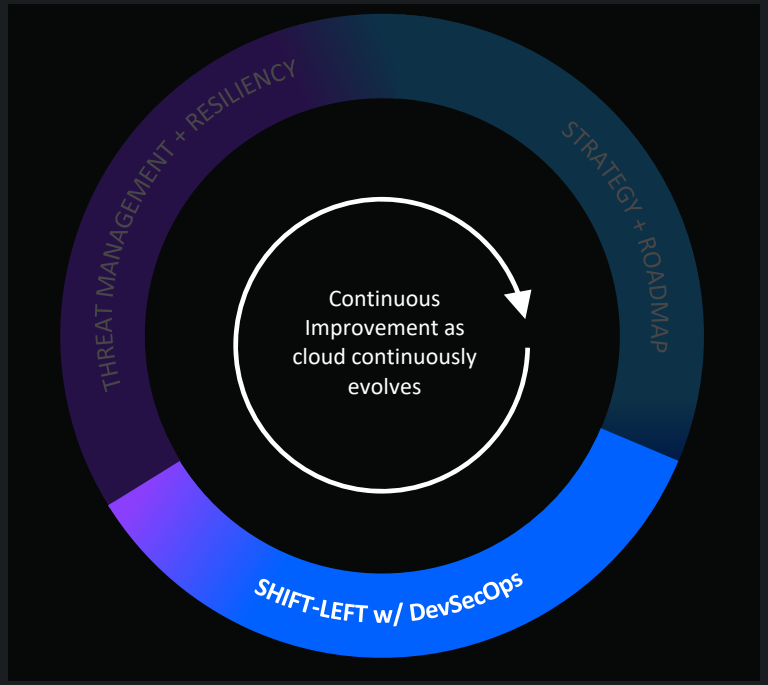
- Risk assessments
- Native, 3rd party, On-prem integration
- Governance and compliance
- Discover / define critical data

Strategy for every layer of the stack

For example:

- Data discovery, classification and access
- IAM transformation
- SOC maturity

Move and build **to the cloud**



Establish Secure-by-design methodology & application development

- **People & Culture:** Secure-by-design training and awareness, secure coding best practices
- Build applications for a secure environment based on secure best practices
- Define security & compliance requirements early

Implement core cloud security controls

Establish cloud specific controls early for:

- network, endpoint, data, and identity

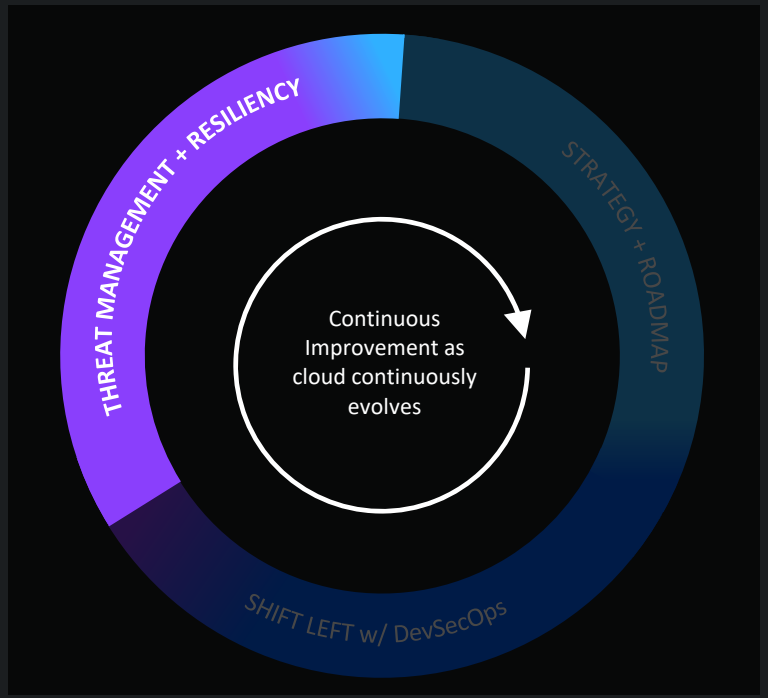
Security Controls Automation

- Automatically implement policies with workload deployment

Continuous application testing

- Application scanning
- Offensive testing

Continuous threat management and resiliency



Centralized Hybrid Environment Visibility & Control

- Collect control status from diverse infrastructure
- Automate day to day policy enforcement

Continuous Compliance Monitoring & Reporting

- Map control status to regulations / standards
- Update controls/policies as regulations and standards change
- Automate reporting and auditing

Optimize Operations and Orchestration

- Continuous feedback for ongoing process improvement

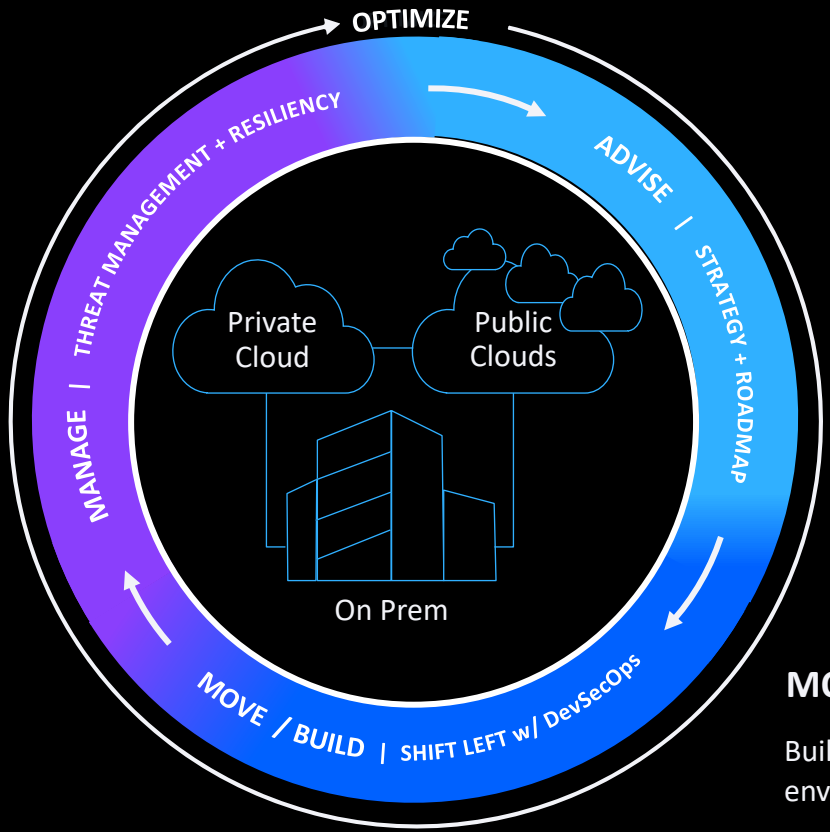
Threat Management

- Monitor and adapt to threat landscape
- Monitor network, user and entity activity to detect attacks
- Eliminate false positives
- Develop a well-documented, communicated, and practiced multi-party Incident Response Plan
- Incident response – containment and remediation
- Disaster Recovery infrastructure

Confidently execute your journey to the cloud

MANAGE

Continuous security and compliance monitoring & threat management



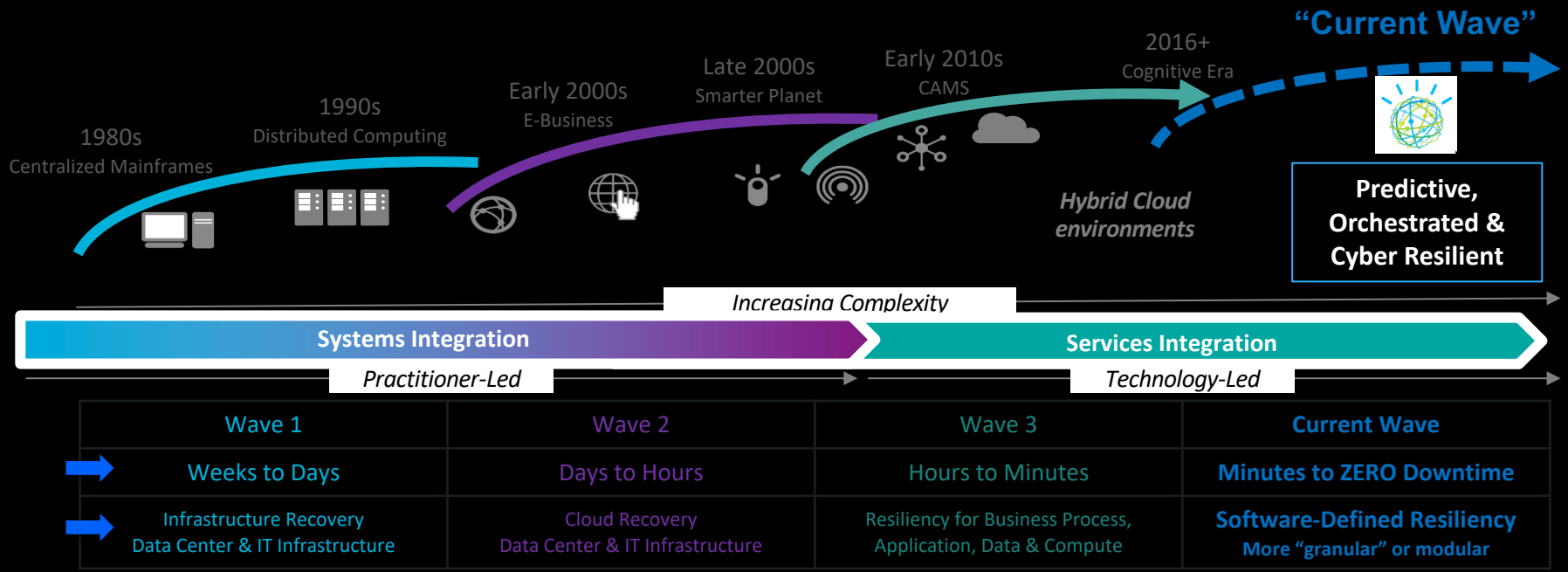
ADVISE

Security & compliance at the core of your cloud transformation strategy and corporate culture

MOVE / BUILD

Building applications based on a secure environment & secure best practices

Resiliency is a business priority triggered by the need for data protection and “always on” service.

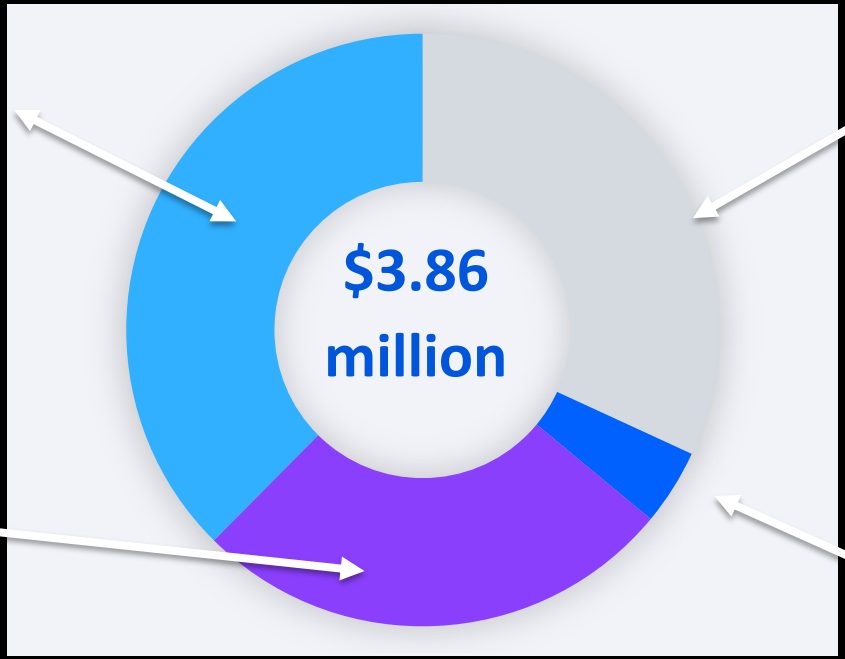


Wave 1	Wave 2	Wave 3	Current Wave
Weeks to Days	Days to Hours	Hours to Minutes	**Minutes to ZERO Downtime**
Infrastructure Recovery Data Center & IT Infrastructure	Cloud Recovery Data Center & IT Infrastructure	Resiliency for Business Process, Application, Data & Compute	**Software-Defined Resiliency** **More “granular” or modular**

The largest component of the total cost of a data breach is lost business.

Lost business cost
$1.45 million
Abnormal turnover of customers, increased customer acquisition cost, reputation losses, diminished goodwill

Ex-post response
$1.02 million
Help desk, inbound communications, special investigations, remediation, legal expenditures, product discounts, identity protection service, regulatory interventions



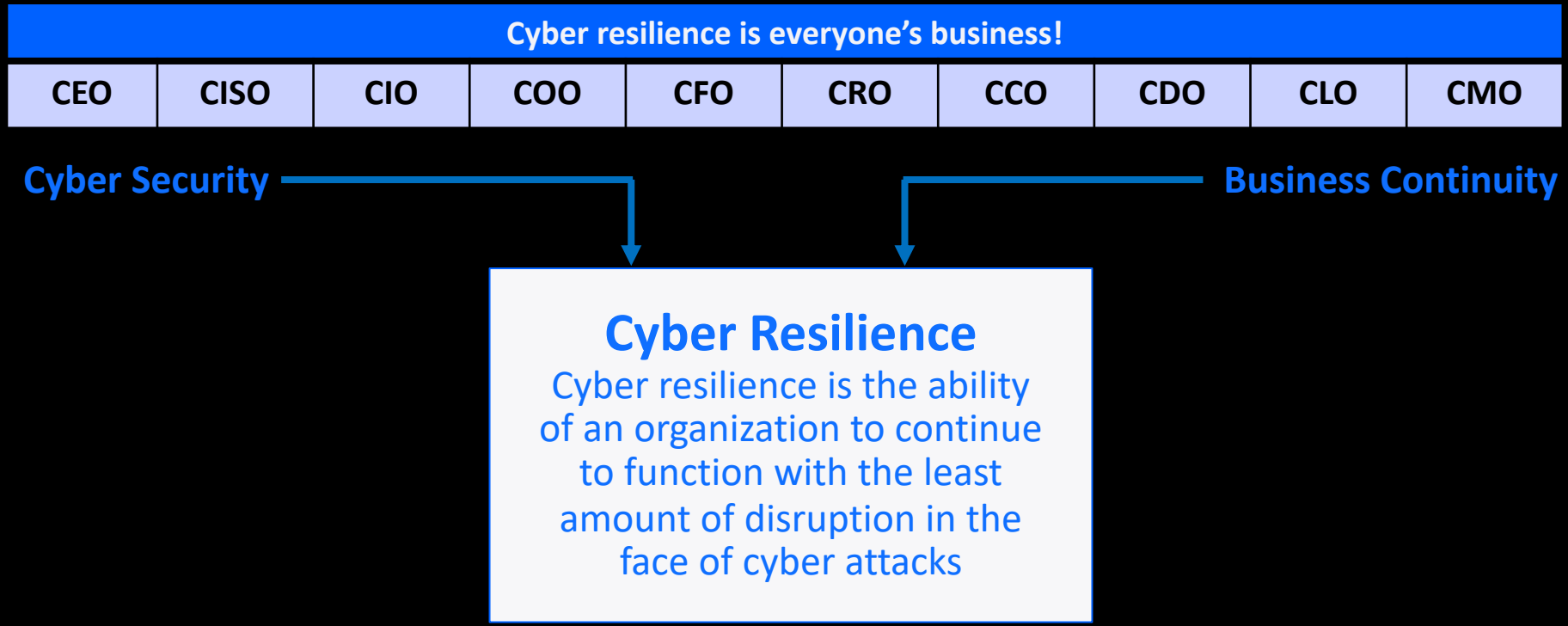
Detection and escalation
$1.23 million
Forensics, root cause determination, organizing incident response team, identifying victims

Notification
$0.16 million
Disclosure of data breach to victims and regulators

Source: 2018 Ponemon Study on Cost of Data Breaches

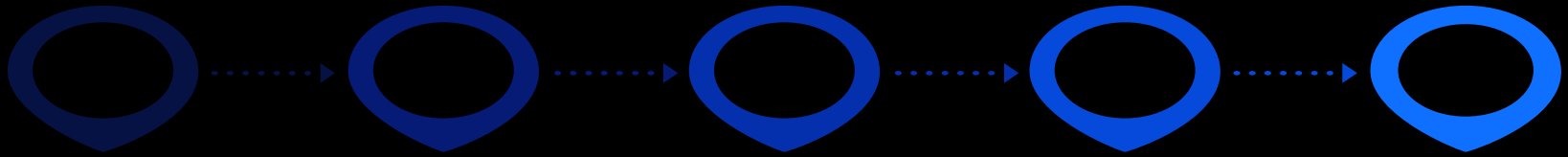
Based on survey respondents from organizations who experienced a data breach from 10K-100K records within the last two years

New threats fuel the need for a **holistic** approach to resiliency & integrated risk management across the enterprise



Cyber Resilience needs a lifecycle approach and relies on five technology elements

Cyber Resilience is the capability to recover business servers very quickly, against cyber outages



I	II	III	IV	V
Orchestration and Automation	**Air-gapped Protection**	**Immutable Storage**	**PIT copies and Data Verification**	**Regulatory Reporting and Assurance**

Comprehensive Cyber Resilience – Doing it Right

Insight

Know your assets and risks – gathering intelligence is the first step.

Prevention

Prevent threats before they wreak havoc – locking the doors goes a long way.

Detection

Spot threats fast – anywhere, anytime using powerful AI and world-class SOCs.

Response

Intelligently orchestrate your response – every minute counts.

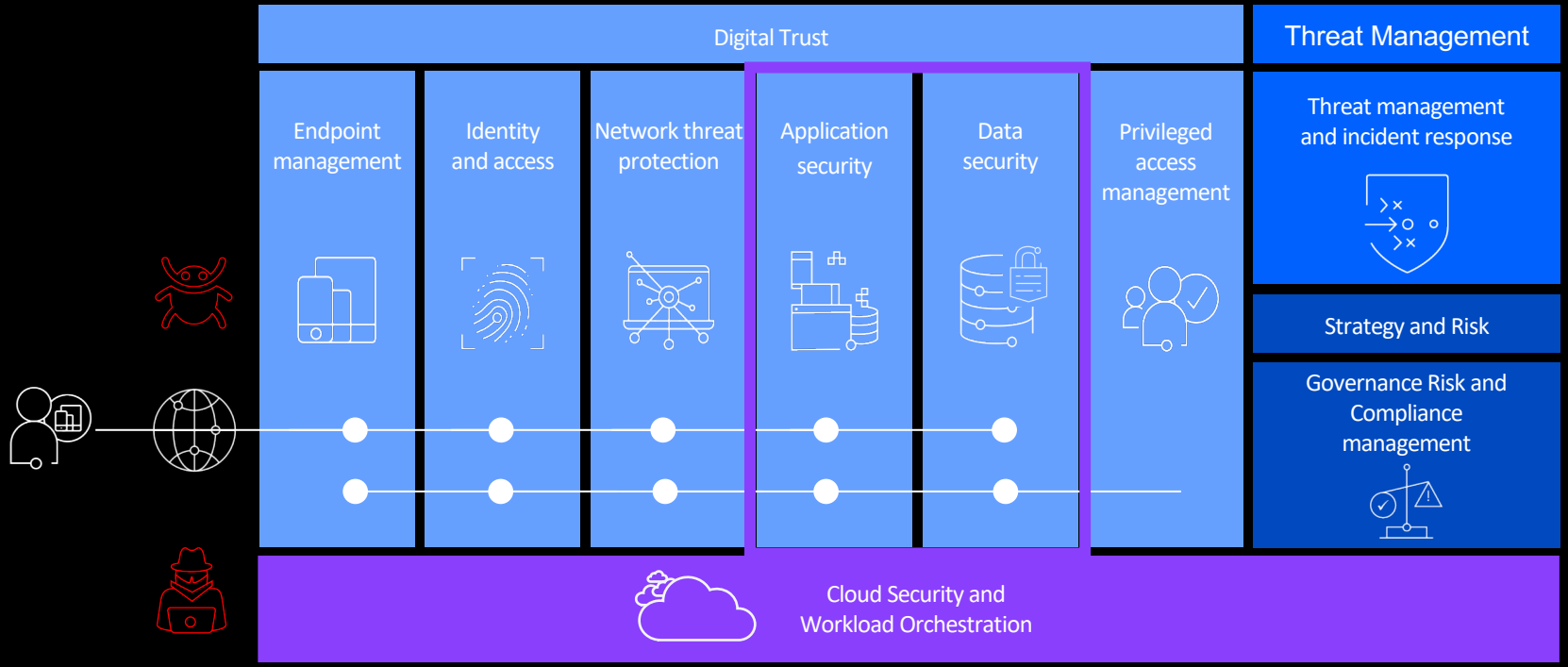
Recovery

Ensure your business is back up and running quickly – a well rehearsed recovery.

Successful Cyber Resilience Requires…

- A comprehensive approach encompassing the full threat management lifecycle and governance framework that drives program maturity.
- An ecosystem of technologies providing best of breed capabilities and force multipliers, such as AI and orchestration, that outpace threats.
- A trusted partner with world class expertise that can keep one step ahead of the threat.

End-to-end security



Where to start in securing your journey to cloud

= Zero Trust*

1 **What and where is my critical data?**

- Data discovery, classification, protection, monitoring

2 **Who has access to my data and systems?**

- Identity Access Management, Governance and PAM

3 **How do I deploy secure workloads?**

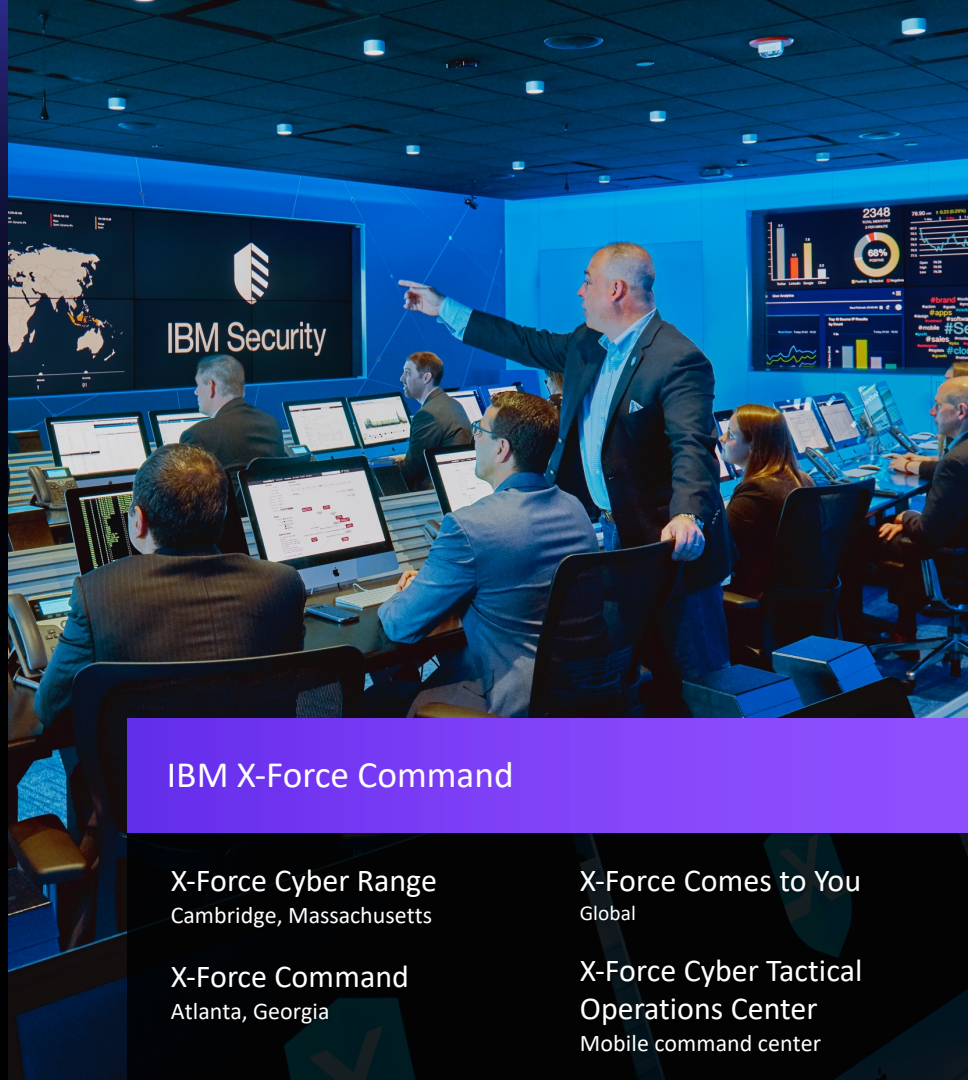
- DevSecOps, microperimeters, policy definition and automation

4 **How do I adapt to threats, respond to attacks and demonstrate compliance?**

- Central visibility and control, analytics, threat hunting and management, CCM, IRP

* kind of

Get business and technical teams actively involved



IBM X-Force Command

X-Force Cyber Range
Cambridge, Massachusetts

X-Force Command
Atlanta, Georgia

X-Force Comes to You
Global

X-Force Cyber Tactical Operations Center
Mobile command center

IBM **Security**

THANK YOU

FOLLOW US ON:

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

lemke@us.ibm.com

IBM