Cybersecurity is Not Cyber Resilience
Hitting Refresh on our thinking

Microsoft
Lead Cybersecurity Architect, Microsoft
“The problem with CISOs, and the entire cyber security field for that matter, is that you keep asking for more money and resources but can’t guarantee or even articulate what I’m buying.”

Un-named CFO
Cybersecurity through a CFO’s Lens

Aware of risks to reputation and bottom line, risk of non-compliance

Show a plan for aggressive cyber risk management
Show a communications plan for risk and incidents (including board and shareholders)
Show how security policies reflect compliance and security aims

Oh, and don’t spend too much money! 😊
Most attackers have a supply chain

You face **ecosystems**, not just hackers and malware

Defenses must address **current** attacker methods
Yes, attack services are inexpensive

**0days** price range varies from $5,000 to $350,000

**Loads (compromised device)** average price ranges
- **PC** - $0.13 to $0.89
- **Mobile** - from $0.82 to $2.78

**Denial of Service (DOS)** average prices
day: $102.05
week: $327.00
month: $766.67

**Proxy** services (evade IP geolocation) prices vary
As low as $100 per week for 100,000 proxies.

**Ransomware:**
- $66 upfront
- Or
- 30% of the profit (affiliate model)

**Spearphishing services** range from $100 to $1,000 per successful account takeover

**Compromised accounts**
As low as $150 for 400M. Averages $0.97 per 1k.
Cybersecurity is a challenging space

Cyber risk is hard to quantify
We try to anyways...
- $141 per breached record (variable)
- Up to $200-310M (1st Q of big incident)

Mitigations are in early days
- Technical mitigations evolving quickly
- Cyber insurance is basic

Doing it wrong is expensive
- Cost of managing 50+ security vendors?

And Getting Harder...
- GDPR requires <72 hour breach report
  - Can you scope a breach accurately that fast?

There is hope!
- Focus on resiliency (vs. being impervious)
  - Prioritize using cost of attack
  - Leverage the cloud for agility

Example: Dofoil outbreak was foiled in milliseconds
Cyber Resiliency

**Integration** - Align and Integrate cybersecurity with business strategy, processes, and initiatives

---

**Mindset**
Adopt a mindset that *assumes compromise* and focuses on:
- Raising attacker costs
- Rapid response/recovery

**Cloud**
Use cloud technologies to
- Tap into community resources and knowledge
- Accelerate innovation (security and productivity)

**Hygiene**
Lower overall risk by
1. Identify well-known risks
2. Steadily burn down list

---

**Key Measures of Success**

<table>
<thead>
<tr>
<th>Cost of Attack</th>
<th>Mean Time To Remediation (MTTR)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Three Major Forces in Digital Transformation

*Adoption Speed impacts Benefit/Risk curve*

- **INCREASE COMPETITIVE ADVANTAGE**
  - REALIZE VALUE FROM NEW TECHNOLOGY
  - INCREASED RISK FROM NEW THREATS

- **DECREASE ORGANIZATIONAL RISK**
  - NEW CONTROLS AND APPROACHES
Three Major Forces in Digital Transformation

Adoption Speed impacts Benefit/Risk curve

- REALIZE VALUE FROM NEW TECHNOLOGY
- INCREASED RISK FROM NEW THREATS
- NEW CONTROLS AND APPROACHES
Machine Learning
Helps overcome human limitations using large datasets

1. Scales out Human Expertise

2. Shines a light in human blind spots
Microsoft Finance - Digital Transformation Areas

Financial Analysis & Reporting
- Revenue Reporting
  - Near Realtime Financial Reporting
  - Scale to meet changing business
- Reconciliation
  - Cost savings
  - Time savings
  - Improved Accuracy

Strategy & Forecasting
- Financial Forecast
  - Predictive Analysis
  - Instant Insights
  - Broader and Deeper Views
- Tax Processing
  - Cost Savings
  - Compliance with New tax rules

Business Process Automation
- Compliance with New tax rules

Risk Management

SOC Reference Operational Model

THREAT INTELLIGENCE
Provide External Context to Inform Decisions
Investigations | Hunting | Leadership | Technical Detections and Defenses

SUCCESS METRIC: Mean Time to Remediation (MTTR)
Across cloud and on-premises

INCIDENT / BREACH MANAGEMENT
Coordinate Data Breaches and Major Incidents with:
Leadership | Legal | Communications | Risk Management | Others

SOC ANALYST
Lead technical incident through lifecycle
Lower Tiers may be automated and/or outsourced to MSSP

DETECT  ›  RESPOND  ›  RECOVER
Mindset
Quick Primer on Security Culture

- Deeply respect truth and facts
- Deeply care about keeping the organization safe
- Limited background in business/communications
  - Many security people incorrectly assume/accept accountability
  - Strained relationship with IT and Business backgrounds
- Prevalent ‘Underdog’ attitude
  - Not involved early in business/risk decision process
Digital is forcing **security** transformation

Requires a modern identity and access security perimeter
Designing for Failure – The Mindshift

THEN

**Reliability:**
Designed not to fail

**Prevent:**
Every possible attack

NOW

**Resilience:**
Designed to recover quickly

**Assume Compromise:**
Protect, detect, and respond along attack phases
Ruin Their ROI
Changing the economics of cybersecurity

ATTACKERS: MAXIMIZE RETURN ON INVESTMENT (ROI) (return may be monetary/political/etc.)
DEFENDERS: RUIN ATTACKER ROI by raising attack cost with protection + rapid response/recovery
MICROSOFT: SIMPLIFY ADVANCED CAPABILITIES across platforms, clouds, and IoT

NOTE: Cost of attack is continuously changing with technical advancement + business model evolution
Cloud
Security Advantages of Cloud Era

TRADITIONAL APPROACH

Security is a challenging and under-resourced function

- Satisfied responsibility
- Partially met responsibility
- Unmet responsibility
- Cloud Provider responsibility (Trust but verify)

CLOUD-ENABLED SECURITY

Cloud Technology enables security to:

- Shift commodity responsibilities to provider and re-allocate your resources
- Leverage cloud-based security capabilities for more effectiveness
- Use Cloud intelligence to improve detection/response/time
Local ML models, behavior-based detection algorithms, generics, heuristics

Metadata-based ML models

Sample analysis-based ML models

Detonation-based ML models

Big data analytics

On March 6, Windows Defender Antivirus blocked more than 400,000 instances of several sophisticated trojans [http://aka.ms/dofoil](http://aka.ms/dofoil)

Other recent cases: [Emotet](http://aka.ms/dofoil) | [Bad Rabbit](http://aka.ms/dofoil)
Hygiene
Hygiene

Hygiene is critically important, but very difficult
Security needs your support
Requires time and focus manage down the “Black Swan Nest” of risk

Start with established guidance
NIST, Center For Internet Security (CIS),
Microsoft, and DHS have built a clear prioritized roadmap to start with

https://aka.ms/CyberHygiene
Summary of Key Recommendations

Measures that directly impact the known attack playbook

**Quick wins: 0-30 Days**

1. Create **destruction-resistant backups** of your critical systems and data
2. Immediately deploy **critical security updates** for OS, browser, & email
3. **Isolate (or retire) computers** that cannot be updated and patched
4. Implement **advanced e-mail and browser protections**
5. Enable host anti-malware and network defenses get near-**realtime blocking responses from cloud** (if available in your solution)
6. Implement **unique local administrator passwords** on all systems
7. Separate and protect **privileged accounts**

**Less than 90 Days**

1. **Validate** your backups using standard restore procedures and tools
2. **Discover and reduce** broad permissions on file repositories
3. Rapidly deploy all **critical security updates**
4. **Disable unneeded** legacy protocols
5. **Stay current** – Run only current versions of operating systems and apps

**Next Quarter + Beyond**

---

https://aka.ms/CyberHygiene
Call to Action
Calls to Action

Hit Refresh on security mindset, adopt “assume compromise”
- It’s ‘normal’ to be attacked successfully
- You **must** manage incidents well and **learn** from them

Support Cloud initiatives (especially for security)

Support and encourage hygiene efforts

Measure Security Success better
- Cost of attack
- Mean time to remediation
References
Microsoft Finance Digital Transformation

Revenue Reporting
- [https://www.microsoft.com/itshowcase/Article/Content/895/Redesigning-our-revenue-reporting-system-for-cloud-architecture](https://www.microsoft.com/itshowcase/Article/Content/895/Redesigning-our-revenue-reporting-system-for-cloud-architecture)

Tax

Forecast