The New Normal: How MSPs can Adapt

Jessvin Thomas, CTO, SKOUT CYBERSECURITY
✓ Contribution from all attendees
✓ Be respectful
✓ Be engaged
✓ Be honest
✓ Be yourself
Please use WebEx Panels to Participate

- This call is being recorded
- To see the slides, click on the WebEx link in your meeting invitation
- You can show panels using the buttons along the bottom of the screen (You may have to hover mouse over them)

Please mute when you aren’t speaking

RAISE HAND by clicking the hand next to your name in the Participants List. Click it again to put your hand down.

Type messages to Host, All Participants or an individual attendee using Chat. Type text, select name or group from list and click Send.
COMPTIA CORPORATE MEMBER BENEFITS EXTEND TO ALL EMPLOYEES:

**RESEARCH**
- IT Industry Outlook
- State of the Channel
- Technology Focused Research (Security, Cloud, IoT, BigData & Much More)
- Industry Focused Research (Managed IT Services, Partner Trends, Channel Conflict)

**CERTIFICATION**
- 15% Off Certification Vouchers
- Employee Certification Validation
- 10% Off Certification Training (On comptia.org store)

**NETWORKING**
- Member Directory: Find other Members through our Membership directory.

**COMMUNITIES AND COUNCILS**
- Ability to Serve in Leadership Positions
- Association Voting Rights

**BRANDING**
- Ability to use CompTIA logo for Promotional Purposes

**EVENTS**
- Free On-Site and Online based training for you and your team
- Unlimited Event Passes for all employees to Channel Con and Communities & Council Forum

**EDUCATION**
- Quick Start Sessions
- Executive Certificate Programs
- Sales Toolkits, Business Tools (Including Templates, ROI Calculators, Case Studies)
- CompTIA Channel Standards

**RETAIL DISCOUNTS (U.S. ONLY)**
- FedEx
- Hertz
- Service800

CompTIA.org/membership
Introducing the CompTIA Cybersecurity Career Pathway
A vendor-neutral pathway for IT professionals to achieve cybersecurity mastery, from beginning to end

Enter where it makes sense
Consider experience and current certifications or course of study

CompTIA A+
CompTIA IT Fundamentals
CompTIA Network+
CompTIA Security+
CompTIA CSA+
CompTIA CASP
Introduce yourself in Chat

• What are you hoping to learn today?

Please type in Chat

• #CompTIAUKCC; #CompTIABenelux and @Comptia_EMEA
Ways to Engage and Stay Connected:

FACEBOOK:
CompTIA Benelux Business Technology Community
CompTIA UK Channel Community

LINKEDIN:
CompTIA UK Channel Community
CompTIA Benelux Business Technology Community

CompTIA Covid-19 Forum
https://covid19.comptia.org/
The New Normal: How MSPs can Adapt

Jessvin Thomas, CTO, SKOUT CYBERSECURITY
The New Normal: How MSPs can Adapt

Jessvin Thomas
President and CTO, SKOUT CYBERSECURITY
Agenda

1. Will this all be over? Is this a new normal?
2. If this is the new normal, how do I best adapt?
3. Having an Offensive and Defensive Plan
4. Cybersecurity concerns are only going to increase in this environment
5. How to be a trusted partner to your customers during this challenging time
This isn’t completely unpredicted
The issue isn’t just about health, it’s about the speed of the dominoes falling.
When you have to, it’s surprising what can be done
Work from home and DR from years to days

**PRE COVID-19 WFH**
- <5% of the workforce was fully remote\(^1\)
- 43% of the workforce worked from home occasionally\(^2\)
- A majority (68 percent) of small-business owners don’t have a written disaster recovery plan\(^3\)

**CURRENT**
- Most of the professional workforce is remote right now
- The top problem is IT setup
  - File access
  - Laptops
  - Video Setup
- Many businesses are still trying to go remote
- Many businesses have gaps that need to be filled by MSPs

---

1. Global Workplace Analytics' analysis of 2018 American Community Service (ACS) data
2. https://dpc.umd.edu/library/research/State%20of%20the%20American%20Workplace%20for%202020.pdf
The New Normal is...

...accelerating trends that were already happening.
Examples

• Work from Home
• Video Meetings and Slack Communication
• Sales process

• IT & Cybersecurity intertwined
What can you do about it

“We need to have an Offensive plan and Defensive plan”

-Aidan Kehoe
CEO and Co-Founder, SKOUT CYBERSECURITY
Defensive

• Take care of your people – Stress, Medical concerns, Readiness from working from home

• Model your business and be extremely conservative
  • Prepare for the long haul

• Looking at salary cost but also software costs and renewals
Offensive

- Packages make sense in the new environment – WfH
- How to onboard faster
- How to provide more flexibility tying cost to revenue

- *Most important, How to help customers be more prepared*
Being Prepared is...

...supporting the trends that were already happening.
Supporting Existing Trends

Characteristics of Most Prepared

- Collaboration
  - Comfortable with chat, video calls, and other forms of distributed communications
- Business Process – HR & Finance
  - Lots of technology enablement in business process
  - Workflow process is digital
- IT - Flexibility and Consumption Based
  - Use SaaS applications
  - Movement to the cloud
- Sales – Movement to inside sales and marketing
  - Comfortable with IP telephony
  - Usage of automated contracts and signature
- Security – Taking a proactive posture
  - Ransomware, business email compromise, compliance
Taking a Proactive Posture in Cyber

The issues are still the same, they are just more impactful.

Having a target state is key
Align with a framework- ISO, NIST, CIS

You don’t have to be perfect!
Have a target state
Five Things To Talk to Your Customer About

1. Pick a framework that covers People, Process and Technology. Point to the framework as way to mitigate the risk — it can be simple.

2. Establish what you want to protect the most. The data and systems YOU care about.

3. Build concentric rings of security around that data.

4. You have to know IF you have a problem, that’s WHY Cybersecurity monitoring your network is ESSENTIAL.

5. You have to take response time down. It’s the difference between a problem getting public or not.
### Simple Framework

<table>
<thead>
<tr>
<th>COSO Controls</th>
<th>NIST Controls</th>
<th>Miscellaneous Controls (GDPR)</th>
<th>(JUL-2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance</td>
<td>Privacy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity &amp; Ethics</td>
<td>Awareness &amp; Training</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Notice of Privacy Rights</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Security</td>
<td>Personal Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Risk Management</td>
<td>Incident Response</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Protection</td>
<td>Security Awareness</td>
<td></td>
<td></td>
</tr>
<tr>
<td>External Communications</td>
<td>IT Security Controls</td>
<td>Mobility &amp; homework submissions</td>
<td></td>
</tr>
<tr>
<td>Risk Management</td>
<td>Protect &amp; Secure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology Support &amp; Help Desk</td>
<td>Endpoint Protection</td>
<td>Policy Controls</td>
<td></td>
</tr>
<tr>
<td>Risk Identification</td>
<td>Business Continuity Plans</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Controls</td>
<td>Identity &amp; Access Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Control</td>
<td>Physical Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quality Control</td>
<td>Program Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>External Monitoring</td>
<td>System Monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring Activities</td>
<td>System Monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal Control &amp; Function</td>
<td>System Monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Awareness &amp; Education</td>
<td>Cybersecurity Awareness</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### COSO + NIST + GDPR

---

### SKOUT's Internal Framework

#### Cyber Health Check-Up

**Scoring Rubric**

<table>
<thead>
<tr>
<th>Service</th>
<th>Risk</th>
<th>Score</th>
<th>Mitigation Factor</th>
<th>Mitigation Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENDPOINT</td>
<td>Not all devices using endpoint</td>
<td>x</td>
<td>4</td>
<td>=</td>
</tr>
<tr>
<td>EMAIL PROTECTION</td>
<td>Using standard spam filters</td>
<td>x</td>
<td>4</td>
<td>=</td>
</tr>
<tr>
<td>2FA/SSO</td>
<td>No 2FA Policy</td>
<td>x</td>
<td>4</td>
<td>=</td>
</tr>
<tr>
<td>FIREWALL/IDS</td>
<td>Using standard firewall</td>
<td>x</td>
<td>4</td>
<td>=</td>
</tr>
<tr>
<td>SECURITY MONITORING</td>
<td>Using standard monitoring</td>
<td>x</td>
<td>4</td>
<td>=</td>
</tr>
<tr>
<td>BACKUP</td>
<td>No backup policy</td>
<td>x</td>
<td>3</td>
<td>=</td>
</tr>
<tr>
<td>THREAT INTEL</td>
<td>No threat intelligence</td>
<td>x</td>
<td>2</td>
<td>=</td>
</tr>
</tbody>
</table>

**Recommendations for Improvement**

**Score Key**

- Below 70: Danger Zone
- 70 - 90: At-risk
- Above 90: Safe Zone

**Total Score:**
How SKOUT Went to the New Normal

**PRE-2018**

- We were primarily in one office
- Having to lock down everything by MAC and IP
- Lots of paper processes and face to face

**POST-2018**

- Design company able to work from a coffee shop
- Be prepared for International
- All SaaS or cloud apps
- Security built in with 2FA
- Everyone gets a corporate laptop with Workspace One and NextGen AV
- Sales processes to sales force
- Workflow to ticketing
- VMWare Workspace One
- Got rid of shared drives
  - Sharepoint, confluence, etc.
- VoIP, Slack, Zoom, Intranet
  - Learned over time that people who weren’t comfortable
  - We waited for people to come to us
The tools were already in place

- Ransomware & BEC accelerated adoption
- GDPR accelerated adoption
- COVID accelerated adoption
- Something else will accelerate adoption
Growing Your MSP means...

...being prepared for trends that were already happening.
Our Outlook

- Cautiously optimistic
- COVID like 2008 recession is going to separate the prepared from unprepared
- Those that can weather the storm also can adapt and grow
- IT & Technology is not going away, adoption will only increase
- Unfortunately that means cybersecurity will not go away, it will only increase
Some things don’t change
Whether COVID Or Otherwise

If you are a trusted partner for your customers and you are there when they need it, you have customer for life.
Some things don’t change
Whether COVID Or Otherwise

If you have trusted partners and technology stack that is there for you when you need it you’ll have a strong business that can adapt.
Questions?
Contact Us

getskout.com

https://www.linkedin.com/in/jessvin/
resources at your fingertips

Introducing the CompTIA App

Features include:
- Key Industry Insights
- Instant Access to CompTIA Content
- Member Directory
- Access to CompTIA Communities & Councils
- Exclusive Thought Leadership
- Tech News From All Over The Globe

Download Now
Visit your App Store and search ‘CompTIA’
Ways to Engage and Stay Connected:

FACEBOOK:
CompTIA Benelux Business Technology Community
CompTIA UK Channel Community

LINKEDIN:
CompTIA UK Channel Community
CompTIA Benelux Business Technology Community

CompTIA Covid-19 Forum
https://covid19.comptia.org/