ARMOR | SECURECON 2019 | DALLAS, TEXAS

HOW CLOUD SECURITY SERVICES FUEL GROWTH FOR MSPS

SCOTT GOODMAN
Partner Business Manager

LEAH MCLEAN
Director of Partner Marketing

DAVID LORTI
Director of Product Marketing

AGENDA

1. What Concerns Leaders Most
2. Cloud Adoption
3. The Threat Landscape
4. Accidental Risk
5. Cybersecurity Skills Shortage
6. How Armor Helps
7. Q & A

SCOTT GOODMAN

Partner Business Manager

Contact me at:
scott.goodman@armor.com

LEAH MCLEAN

Director of Partner Marketing

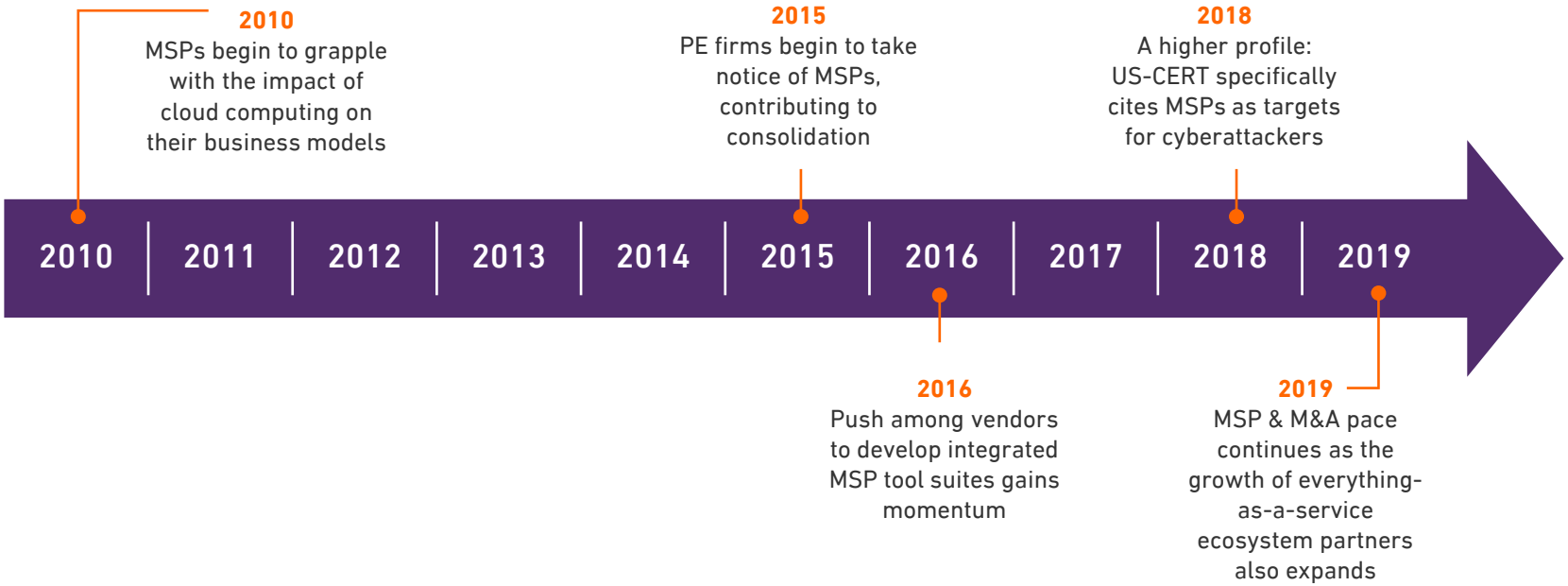
Contact me at:
leah.mclean@armor.com

DAVID LORTI

Director of Product Marketing

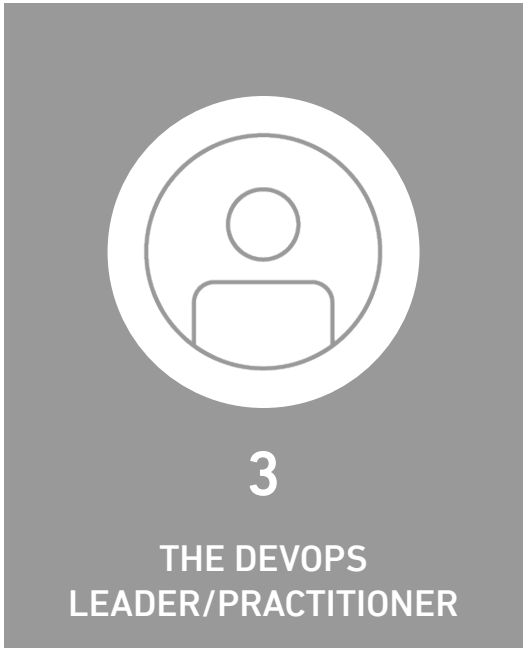
Contact me at:
david.lorti@armor.com

MSP EVOLUTION TIMELINE

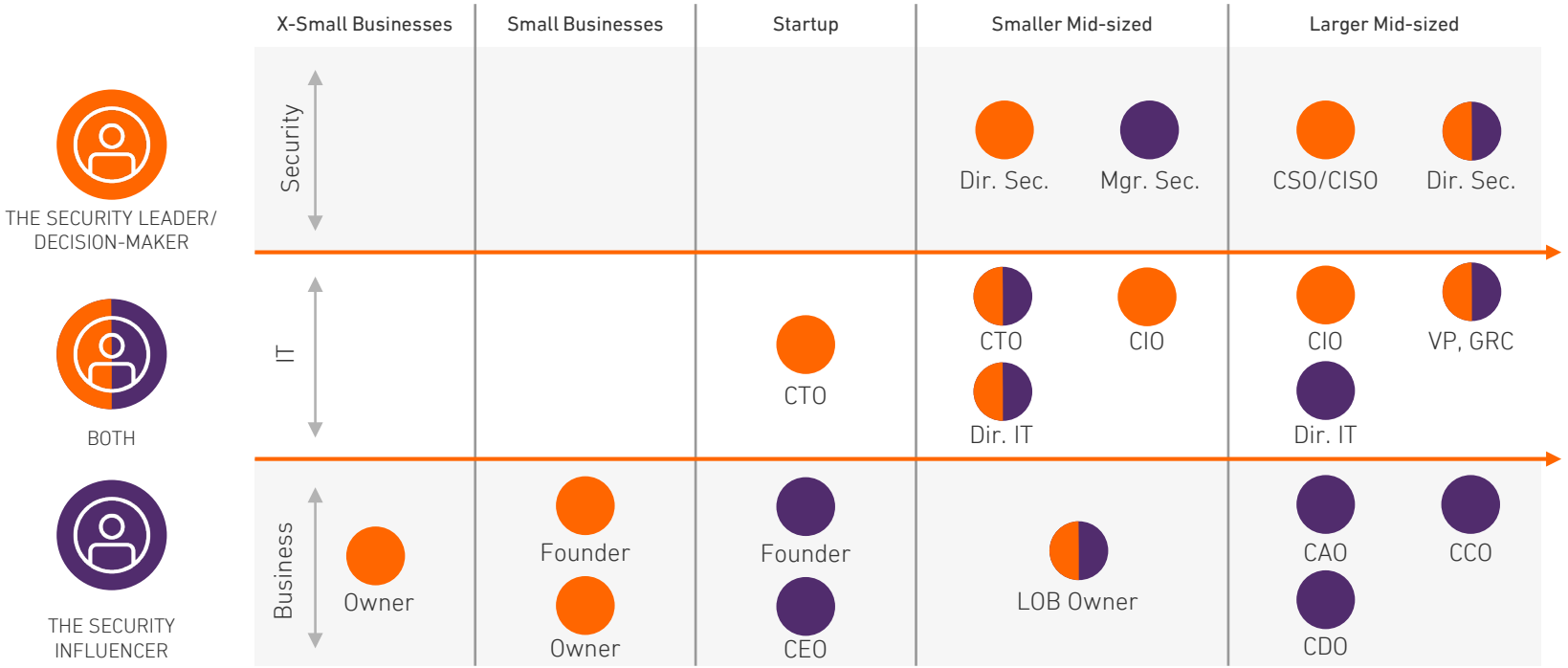


WHAT CONCERNS LEADERS MOST

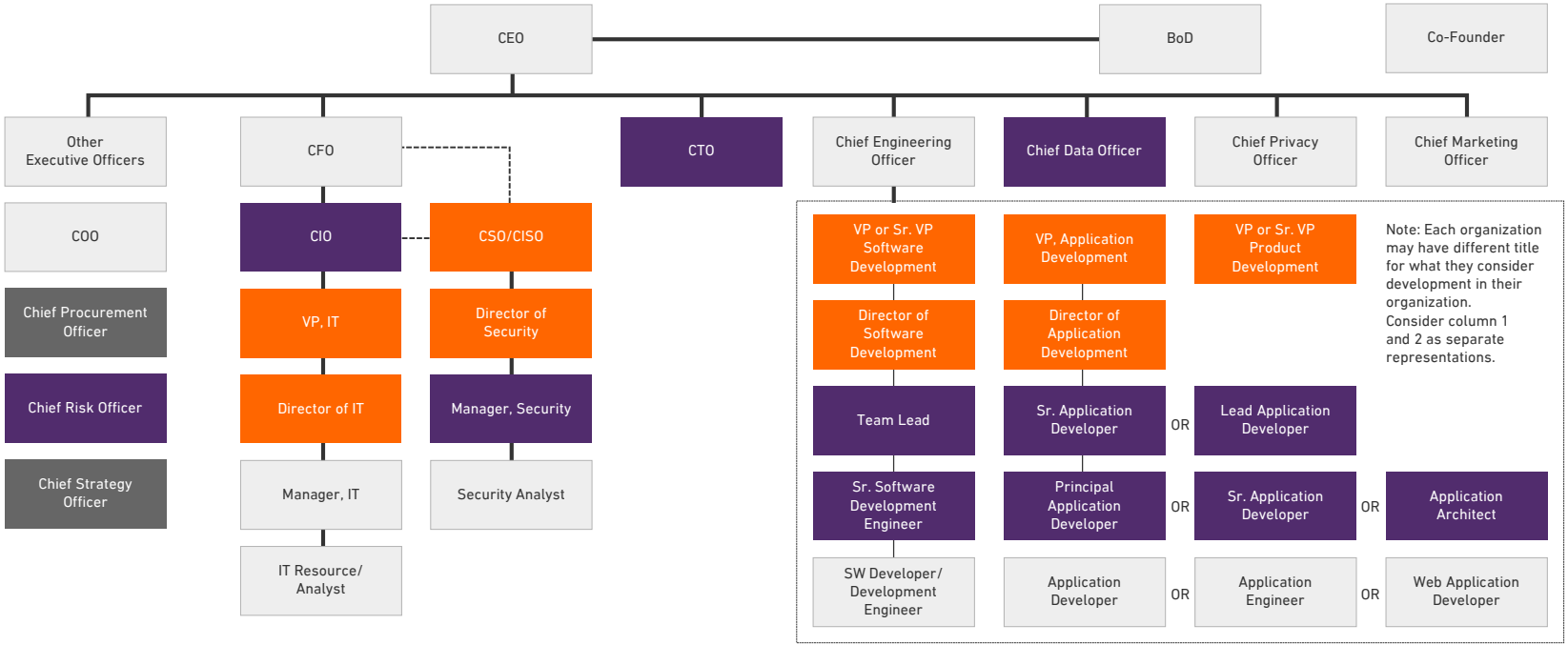
YOUR TARGET AUDIENCE IS EXPANDING



SECURITY PERSONAS



WHO WE ARE TARGETING



THE FUTURE OF THE CISO

It is not simple to evolve from the kind of cloistered, poorly communicating security department that has characterized many organizations into an operation that is fully engaged and adapted. CISOs have to step outside of the security domain and see what value they can add throughout the organization.

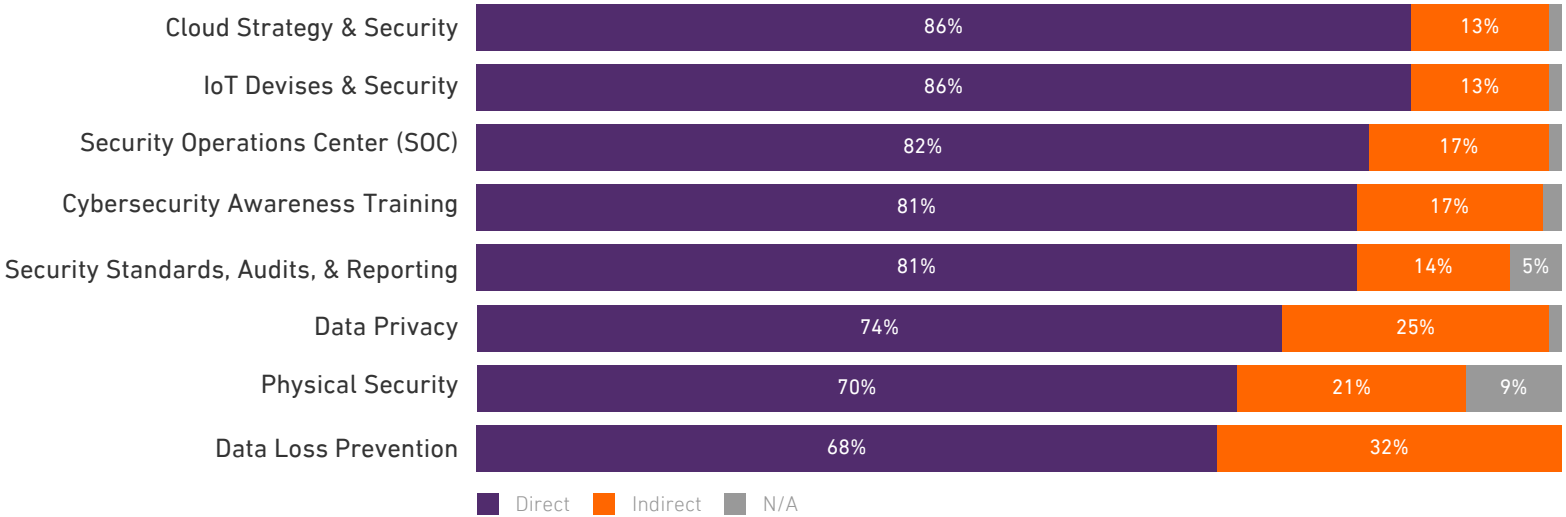
1. How can cybersecurity help generate, protect, and ensure revenue?
2. How can cybersecurity help retain existing customers?
3. How can cybersecurity help differentiate against competitors?
4. How can cybersecurity drive operational efficiencies and effectiveness?

Tomorrow's CISOs will have to be on intimate terms with every aspect of the organization.

— DORA. (2019). *Accelerate State of DevOps 2019.*

Source: "The Evolving Role of the CISO: From Risk Manager to Business Enabler," SecurityRountable.org – July 31, 2018

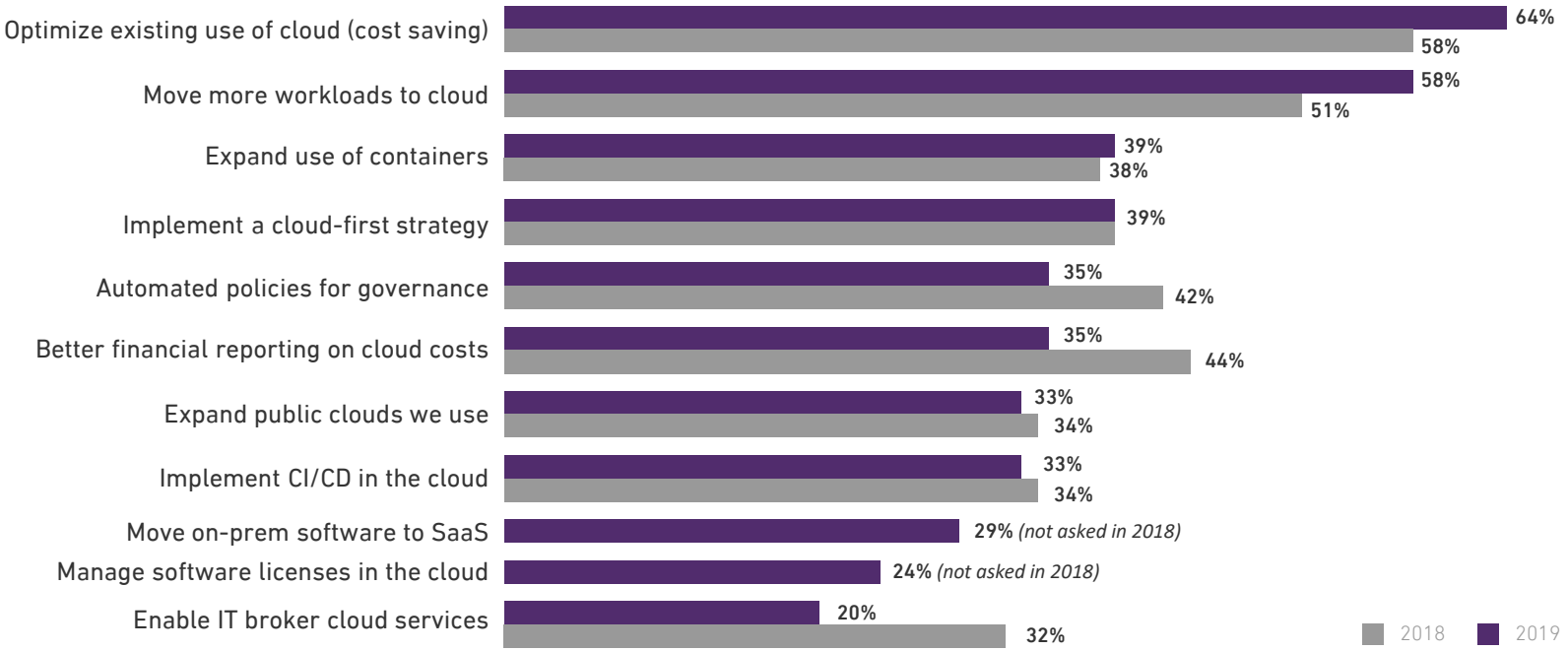
RESPONSIBILITIES/PRIORITIES FOR CISOs



Top 3 priorities should align with business/IT projects. An expanding attack surface demands SOC operations be scaled to effectively support.

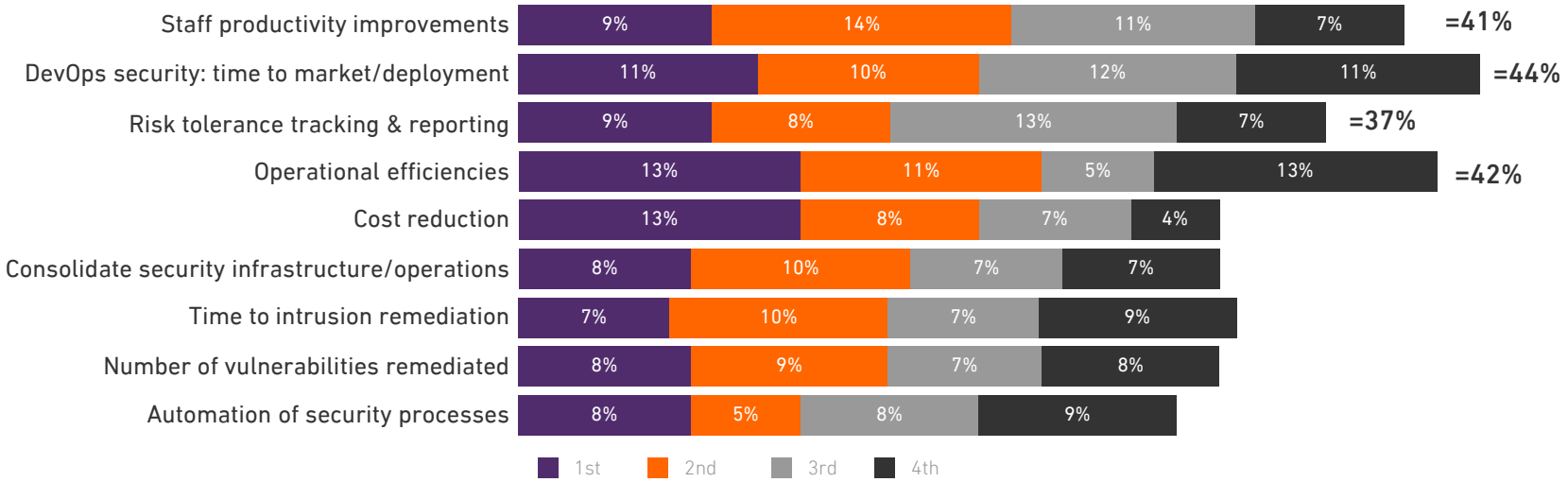
Source: "The CISO and Cybersecurity REPORT A Report on Current Priorities and Challenges," Fortinet – April 2019

TOP CLOUD INITIATIVES



Source: "RightScale 2019 State of the Cloud Report from Flexera," Flexera - 2019

RESPONSIBILITIES/PRIORITIES FOR CISOs

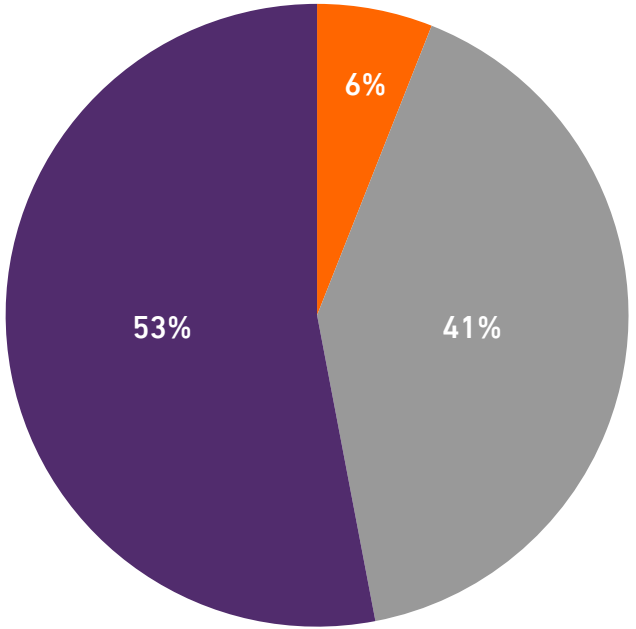


Top metrics imply a strong focus on risk and driving efficiencies to effectively manage it. This includes recognition of risk introduced by application development teams.

Source: "The CISO and Cybersecurity REPORT A Report on Current Priorities and Challenges," Fortinet – April 2019

CISOs' USE OF MSSPs

Organizations want security partners, not replacements. Only a small percent actually outsource most security functions (based on organizations with 2,500+ employees).

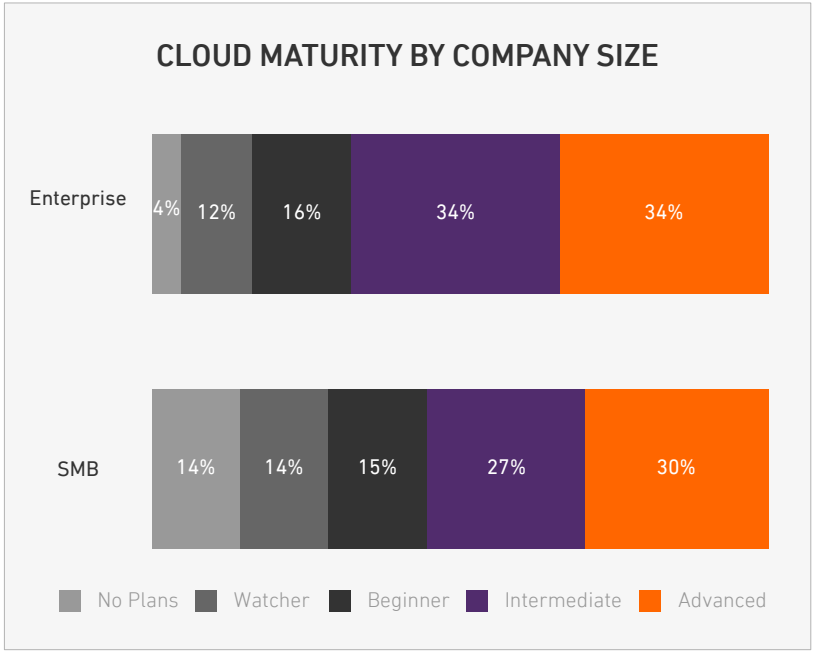


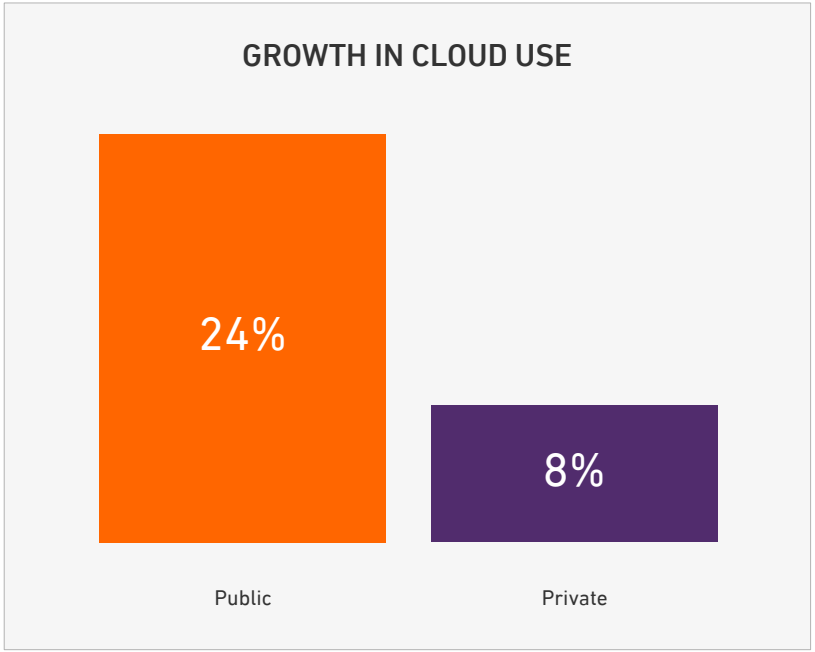
- Yes, we outsource a majority of security functions.
- Yes, we partner for implementation & mgmt. support.
- No, we handle everything in-house.

Source: "The CISO and Cybersecurity REPORT A Report on Current Priorities and Challenges," Fortinet – April 2019

CLOUD ADOPTION

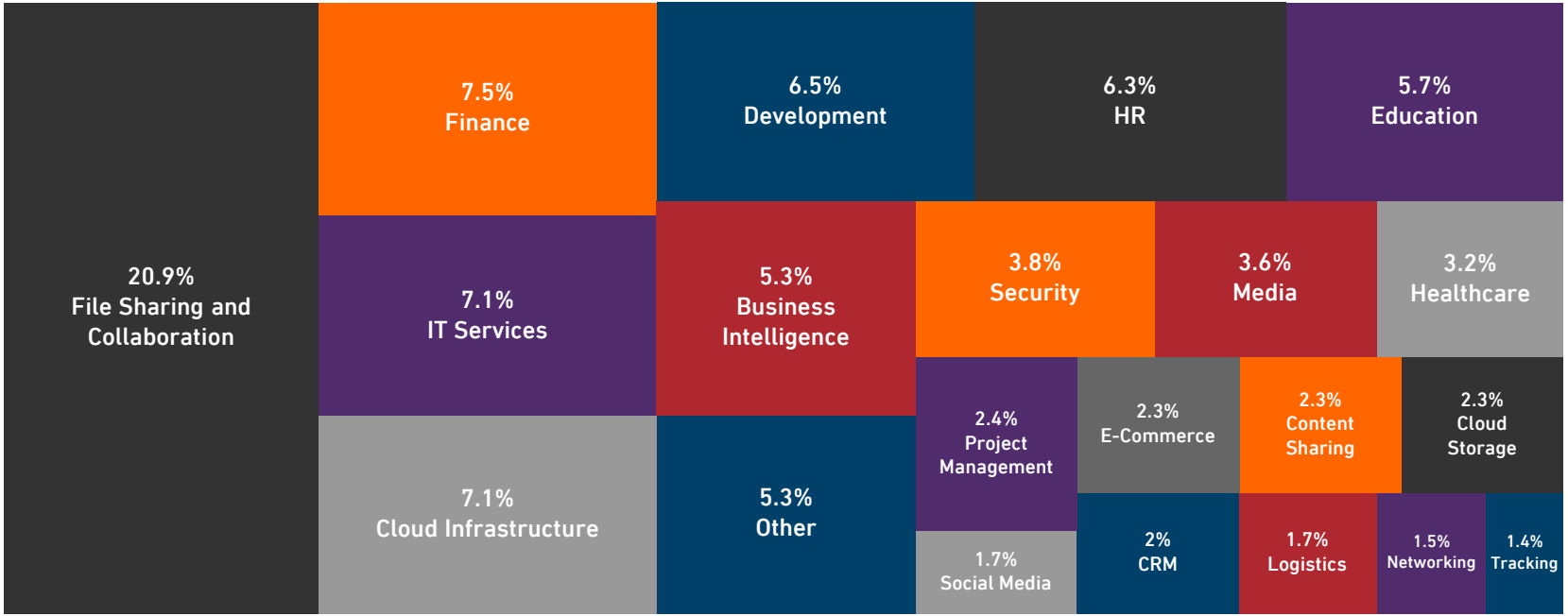
CLOUD MATURITY AND GROWTH





Source: "RightScale 2019 State of the Cloud Report from Flexera," Flexera - 2019

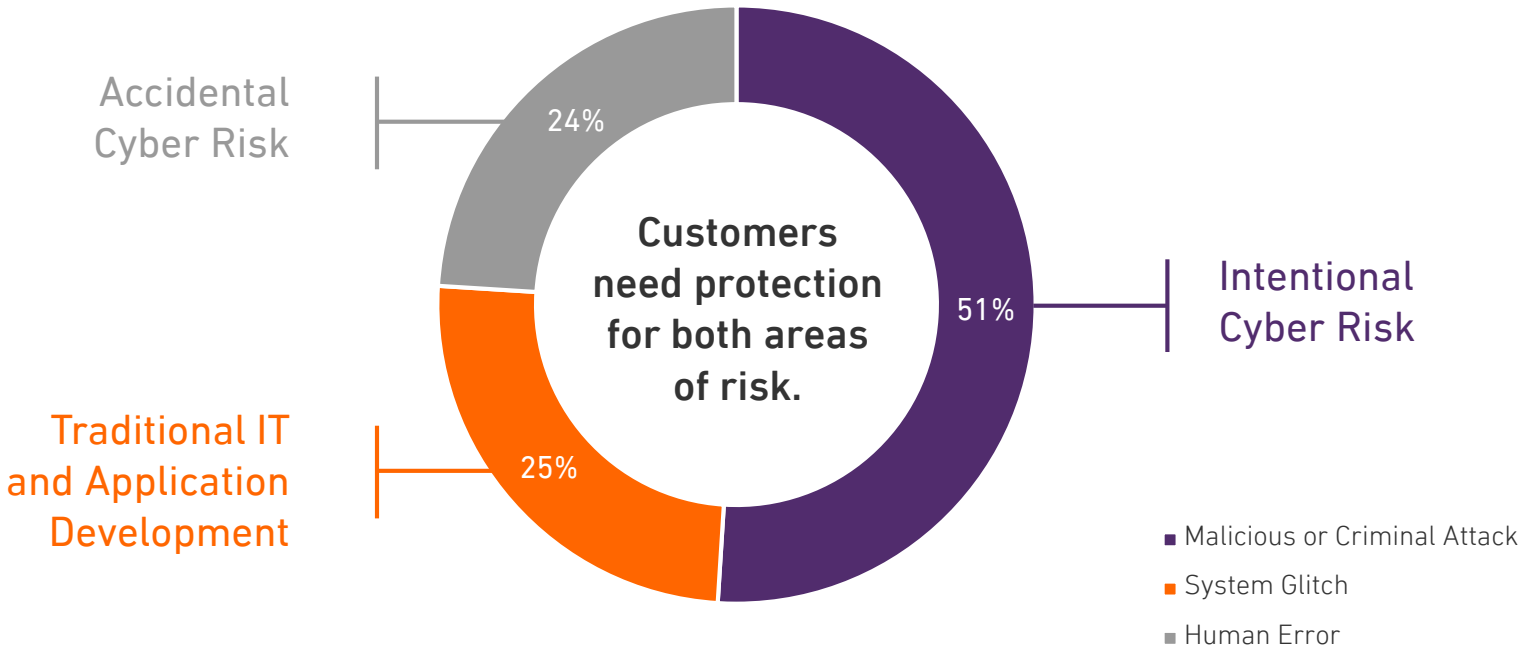
CLOUD USAGE BY CATEGORY



*Source: "Cloud Adoption and Risk Report," McAfee – 2019

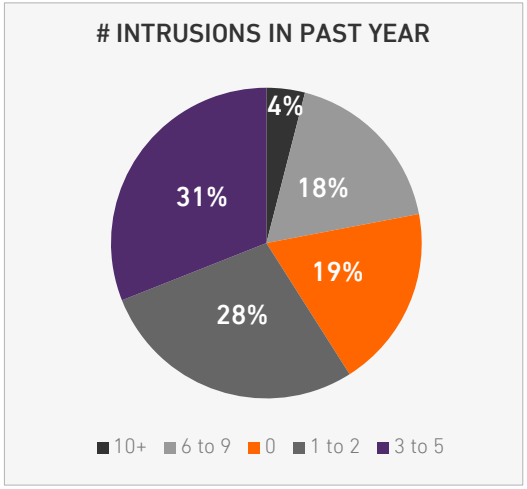
THE THREAT LANDSCAPE

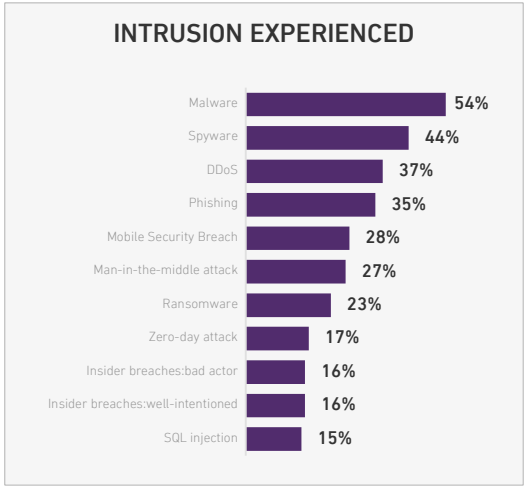
ROOT CAUSES OF DATA BREACHES



Source: "2019 Cost of a Data Breach Report," Ponemon Institute - 2019

CHALLENGES ARISING FROM AN INCREASED ATTACK SURFACE

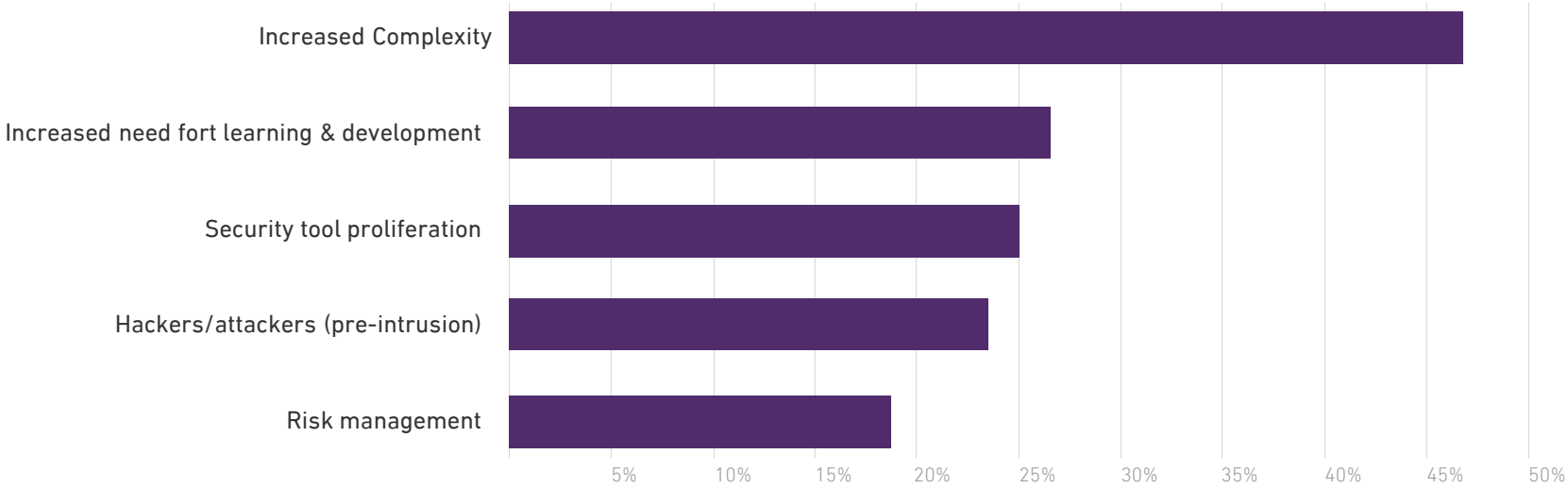




The risk and its potential impact are very real. And though ransomware has garnered significant attention, traditional malware threats are much more prevalent.

Source: "The CISO and Cybersecurity REPORT A Report on Current Priorities and Challenges," Fortinet – April 2019

CHALLENGES ARISING FROM AN INCREASED ATTACK SURFACE



CISOs are clearly very concerned for complexities arising from expansion to the cloud, IoT and other initiatives that expand the attack surface. As a result, they are likely to look for solutions that solidly address this complexity.

Source: "The CISO and Cybersecurity REPORT A Report on Current Priorities and Challenges," Fortinet – April 2019

ACCIDENTAL RISK

TO ERR IS HUMAN, BUT COSTLY

MISCONFIGURATIONS, "HONEST MISTAKES," AND CARELESSNESS IS FUELING "ACCIDENTAL" CYBER RISK ACROSS ORGANIZATIONS.

14 Enterprise organizations have an average of 14 misconfigured IaaS/ PaaS instances running at one time.*

920M Thirteen major accidental (no threat actor involved) data exposures since 2017 exposed nearly one billion records.**

5.5% 5.5% of AWS S3 buckets have world read permissions, making them open to the public.*

8/13 The number of incidents where data was exposed by an affiliate, partner, or customer of a larger organization.**

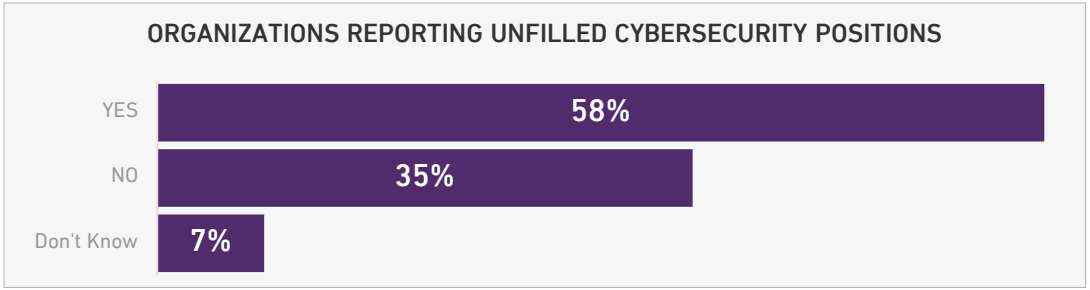
*Source: "Cloud Adoption and Risk Report," McAfee – 2019. **Source: "Naked Data," Armor - 2019

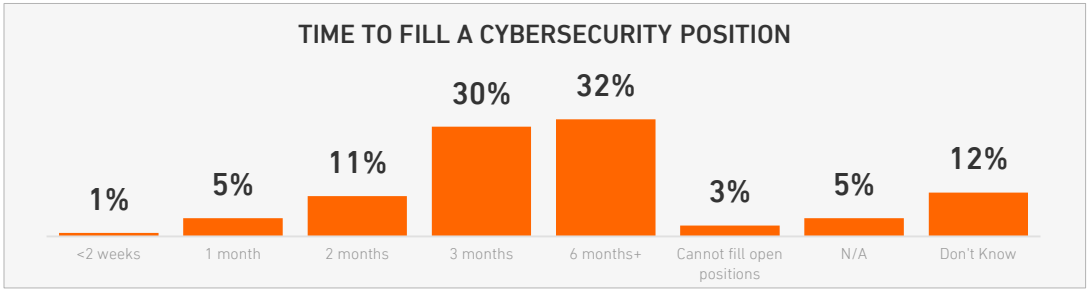
CYBERSECURITY SKILLS SHORTAGE

CYBERSECURITY TALENT

Customers needs your help because their ability to hire and retain strong cybersecurity talent remains an ongoing and frustrating challenge.

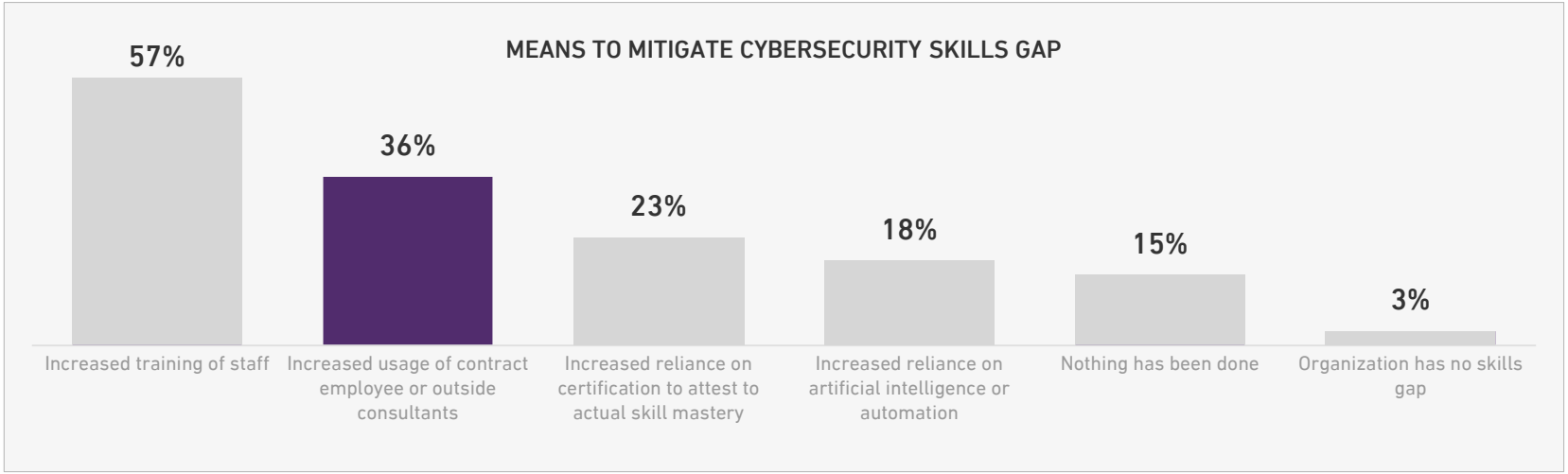
Don't expect the cybersecurity skill shortage to be solved anytime soon.





Source: "State of Cybersecurity 2019," ISACA - 2019

MITIGATING THE SHORTAGE



Organizations will increasingly look to MSPs to expand their coverage and provide security and compliance protections.

Source: "State of Cybersecurity 2019," ISACA - 2019

HOW ARMOR HELPS

UNDERSTANDING FIT

Traditional Institutions/Services

Education
- Training Providers
- Colleges/Universities

Financial Services Firms
- Banks
- Credit Unions
- General non-technology financial services

Government (Fed/State/Local)

Insurance Providers

Real Estate Services
- Brokerages
- General non-technology services

Utilities

Consumer Goods (when have stronger urgency)

Education Technology Providers

Legal Services
- Law Firms
- Legal Technology Providers

Healthcare Services
- Clinics
- Hospitals
- Doctors offices
- General non-technology healthcare services

Tech/Data-Driven

Financial Technology Providers

General Technology Providers (all industries)
- SaaS
- "Platforms"
- "Software"

General Technology Services
- App Development
- Software Development
- IT Services (Includes managed)
- Technology Consulting

Healthcare Technology Providers

Marketing Services (Digitally-driven)

Other Digitally-driven services providers (where digital IP is their business)*

Openness to public cloud usage.

UNDERSTANDING FIT – CLOUD/ON-PREMISE/HYBRID

Tech-driven and data-driven companies share a focus on their core competencies and/or application development while minimizing technical debt.

Traditional Institutions/Services

Consumer Goods
(when have stronger urgency)

Education Technology Providers

Legal Services
- Law Firms
- Legal Technology Providers

Healthcare Services
- Clinics
- Hospitals
- Doctors offices
- General non-technology healthcare services

Tech/Data-Driven

Financial Technology Providers

General Technology Providers (all industries)
- SaaS
- "Platforms"
- "Software"

General Technology Services
- App Development
- Software Development
- IT Services (Includes managed)
- Technology Consulting

Healthcare Technology Providers

Marketing Services (Digitally-driven)

Other Digitally-driven services providers (where digital IP is their business)*

Includes much larger entities where Armor solutions can help with a similar use case.

UNDERSTANDING FIT – SECURE HOSTING

Traditional Institutions/Services

Education
- Training Providers
- Colleges/Universities

Financial Services Firms
- Banks
- Credit Unions
- General non-technology financial services

Government (Fed/State/Local)

Insurance Providers

Real Estate Services
- Brokerages
- General non-technology services

Utilities

Consumer Goods (when have stronger urgency)

Education Technology Providers

Legal Services
- Law Firms
- Legal Technology Providers

Healthcare Services
- Clinics
- Hospitals
- Doctors offices
- General non-technology healthcare services

Includes much larger entities where Armor solutions can help with a similar use case.

Organizations tend to be subject to one or more major compliance frameworks, have a very strong sensitivity to protecting applications and data, and more averse to public cloud usage.

ARMOR

HOW ARMOR HELPS

WHO	EXECUTIVES	SECURITY PROS	DEVELOPERS
WHAT	SECURITY		COMPLIANCE
	ELASTIC	SCALE	SIMPLICITY	SPEED	TRUST	VALUE	VISIBILITY
HOW	PLATFORM → TECHNOLOGY		PEOPLE + PROCESS
WHERE	SECURE HOSTING	ON-PREMISE	CLOUD	HYBRID	MULTI-CLOUD

Q & A

SCOTT GOODMAN
Partner Business Manager

LEAH MCLEAN
Director of Partner Marketing

DAVID LORTI
Director of Product Marketing

ARMOR | SECURECON 2019 | DALLAS, TEXAS

THANK YOU.

WWW.ARMOR.COM

THE COST OF A CLOUD MISCONFIGURATION

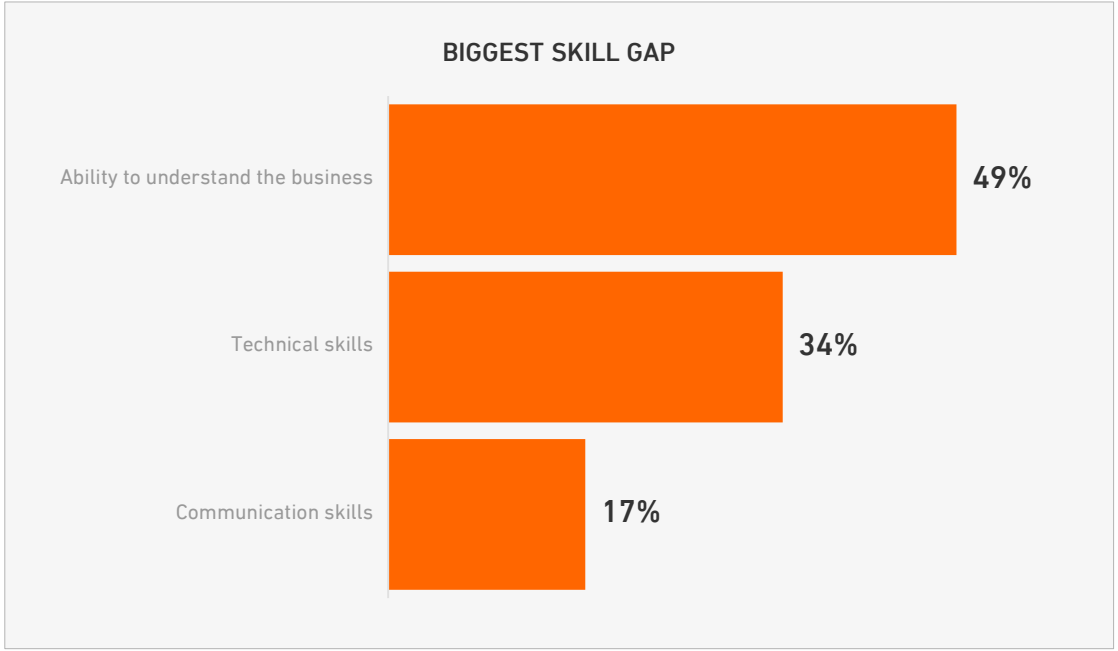
COSTS ASSOCIATED WITH RISKS: $148 PER EXPOSED RECORD, UPWARD OF A COMBINED $57B.

DETECTION & ESCALATION	NOTIFICATION COSTS	POST DATA BREACH RESPONSE	LOSS OF BUSINESS COST
Detecting and reporting a breach to the appropriate personnel in a timely manner. Forensic and investigative activities, audit services, crisis management, and communications teams	**Properly notifying data subjects whose information has been compromised.** Hard costs of paper, equipment, labor, communications with regulators and outside experts.	**Helping individuals affected by the breach to communicate with the company.** Help desk activities, credit report monitoring and identity protection services, issuing new accounts or credentials, legal expenses, product discounts, and regulatory fines.	**Overall cost to the business.** Accounts for losing customers, system downtime, business disruption, and reputation damage.

KNOWING YOUR CUSTOMER'S BUSINESS IS AN ADVANTAGE

Your close relationships to your customers can fuel cross-sell opportunities as they trust you with their most important assets.

Use your relationships to have consultative engagements on security and compliance and win more wallet.



Source: "State of Cybersecurity 2019," ISACA - 2019