BOSTON CONSULTING GROUP

BCG PLATINION

Are you adequately protecting against increasing COVID-19 cyber threats?

Michael Coden, Managing Director, Global Lead Cybersecurity Practice
Coden.Michael@bcg.com

BCG PLATINION

MARCH 2020

Our involvement in international standards, policies, regulations, academic, and industry product research gives us unique insights for cybersecurity

Private Sector

We are partnered with the World Economic Forum to engage global leaders on promoting cyberresilience

Public Sector

We are working with multiple governments, including the US NIST, to set cyber policy and standards

Technology Providers

We have worked with 1/3 of the largest security tech vendors to help them set their product strategies[1]

Academic Institutions

We are partnered with MIT's inter-disciplinary consortium to apply top cyber research to busi-ness challenges

Industry Associations

We engaged with the Bank Policy Institute and it's members to help harmonize 20+ cyber regulations

Cyber Insurers

We are exploring the potential for cyber insurance with the leading international think tank of the insurance industry

Law Enforcement

We helped create a joint taskforce where industry and Interpol collaborate on cybercrime

Global Standards

We are providing thought leadership in the development of global cyber standards and frameworks

1. Vendor market share according to Gartner's Security Software Market Share top 30 vendors, 2016
Source: BCG

As companies shift millions of staff to remote working and expand their technology stack, they are increasing their attack surface

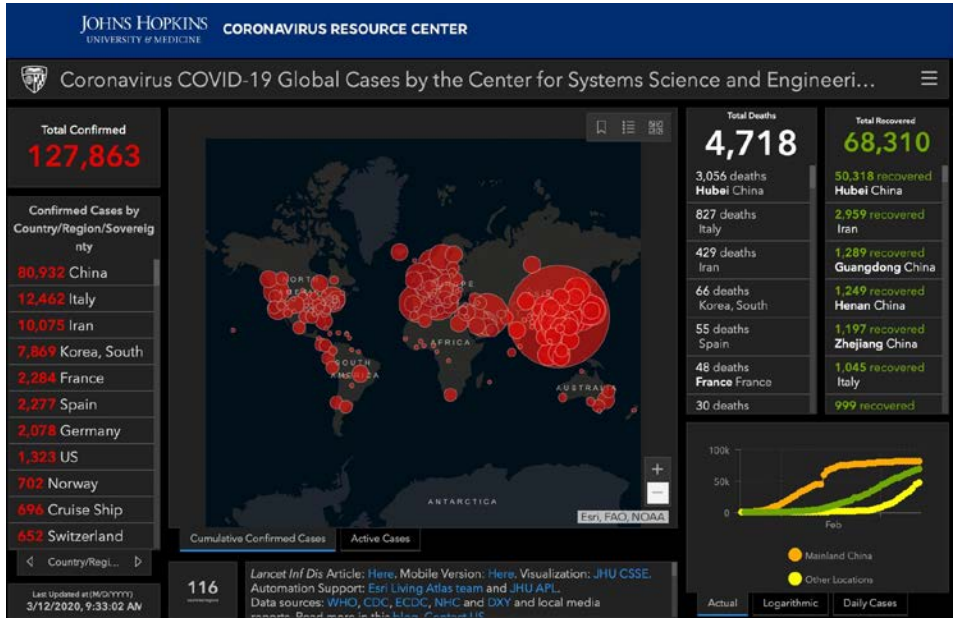
Simultaneously cyber attackers are using COVID-19 fears to take advantage of a newly mobile workforce

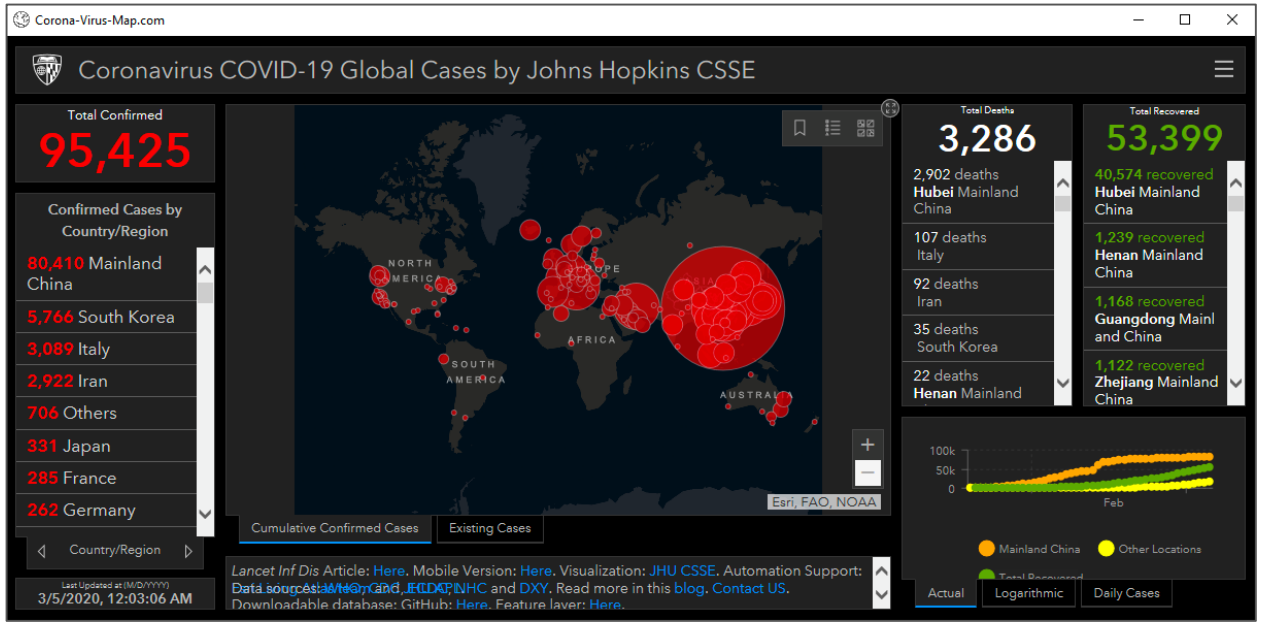
7 things you should do to address new Cyber risks occurring from current COVID-19 crisis

1. Check that your technology supports secure remote working
2. Secure your remote work environment
3. Embed cyber into your crisis & business continuity plans
4. Increase awareness of the additional cyber risks when working remotely
5. Establish protocols and required behaviors for secure remote working
6. Enable crisis management teams to work in a secure manner
7. Update identity & access security measures to account for new threats

Website provides actual & accurate data on COVID-19 …

… Phishing emails include a link to software duplicating the website and installs infectious malware





Cybercriminals are targeting the families and home networks of C-Suite individuals to get easy access and pivot to corporate – at home - endpoints

Source: Website from Johns Hopkins University, Coronavirus Resource Center, https://coronavirus.jhu.edu/map.html; Live Corona Map Used to Spread Malware, Krebs on Security, 12 March, 2020, https://krebsonsecurity.com/2020/03/live-coronavirus-map-used-to-spread-malware/

Migrating workforce operations from office to remote increases cyber security threats & risks

- Remote and mobile infrastructures greatly increase **cyberattack surface**
- **Critical assets** are now accessible remotely
- Previously reliable security processes may **no longer be effective**
- Employees working remotely face **new unfamiliar threat vectors**, such as phone scams, business phishing at home, credential theft, and more
- **Critical support systems** such as IT & Security Operations may be
  - quarantined & need to function remotely or
  - staff is hospitalized and unavailable to respond to a cyberattack
- **Backups and restoration operations** may become unavailable due to pandemic travel restrictions and overloaded network failures
- **Video and voice conferences** can be infiltrated by unauthorized parties

Update your cybersecurity focus

1. Enabling robust remote access technology
2. Defining new remote operational processes
3. Creating employee awareness & training programs
4. Deploying secure video and voice conferencing tools
5. Expanding employee help desks & support

Include cyber preparedness in your COVID-19 crisis management plan

Workers are worried and afraid

Begin working remotely – isolation

-Backups
-Restores
-Location

- Increased attack surface
- Insider threat increase
- Time & Location threat

- Weak network security
- Spear phishing suceptibility
- Lack of training awareness

- No hardwired connectivity
- Remote worker impersonation
- Help desk impersonation

- Can tools be used remotely?
- Are backup personnel trained?

Worker & help desk Authentication is critical

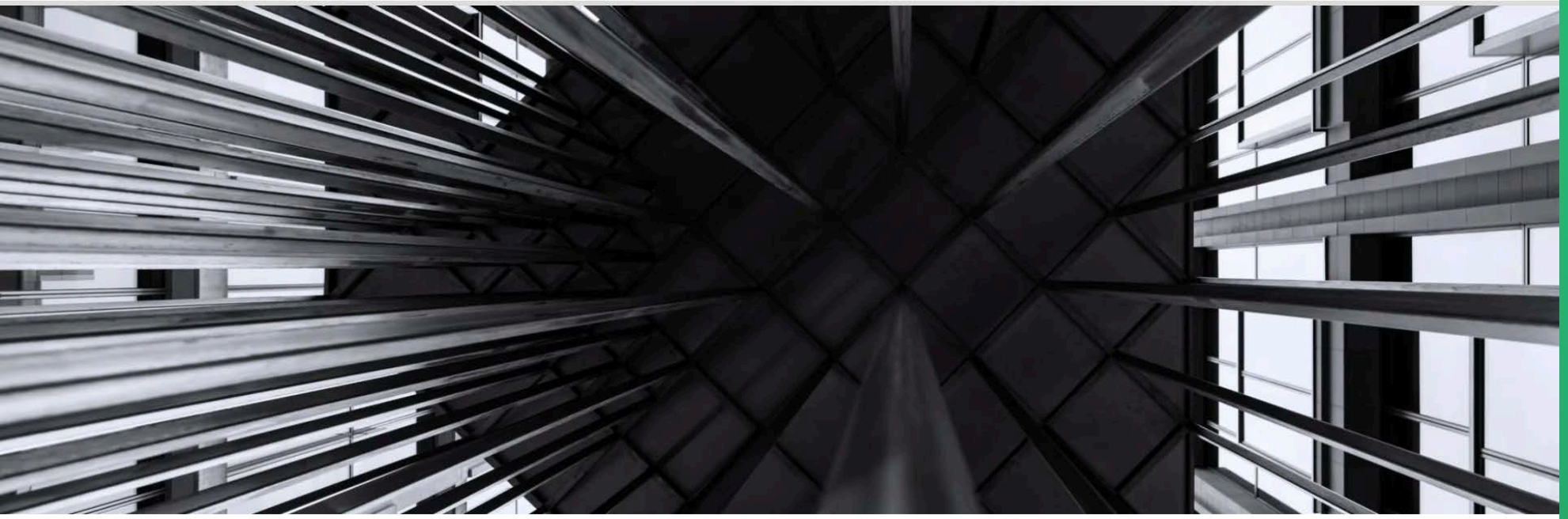
Cyber attackers exploiting remote work & COVID-19 fears

Family members at home are vulnerable

IT & Cyber support staff working remotely or unable to work

Conference call intruders

- Use passwords
- Take attendance



RELATED EXPERTISE: TECHNOLOGY & DIGITAL, TRANSFORMATION OF THE TECH FUNCTION, BIG DATA & ADVANCED ANALYTICS

Managing the Cyber Risks of Remote Work

MARCH 20, 2020

By Michael Coden, Karalee Close, Walter Bohmayr, Kris Winkler, and Brett Thorson

Article

https://www.bcg.com/publications/2020/covid-remote-work-cybersecurity.aspx

Detailed instructions and checklist

https://connect.bcg.com/data/uploads/sites/1304/2020/03/COVID-19-Cybersecurity-for-remote-workforce-v20200318.pdf

Organizations must implement a range of actions to operate securely during a pandemic

Actions and Rationale

1	Check that your Tech supports secure remote working	Establishes base-level mobile workforce abilities
2	Secure your remote work environment	Protects against cyber attacks and strengthens ability to operate virtually
3	Embed cyber into crisis & business continuity plans	Allows core operations to continue without full services and technologies
4	Increase awareness when working remotely	Ensures workforce understands threats and how to work remotely
5	Set expectations for secure remote working	Establishes clear protocols and behaviors for remote working
6	Enable crisis mgmt. teams to work in a secure manner	Aligns internal and external stakeholders to operate securely
7	Update identity & access security measures to account for new threats	Provides tailored security for key roles and groups (based on threats)

Source: BCG

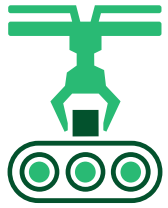
Organizations are facing a number of cybersecurity imperatives

Supply chain cyber risk

- 3rd and 4th party dependency management – they're all part of a single attack surface
- Advanced security for most critical suppliers, providers, & systems (BCG's work with NIST)
- Ensuring product Data Integrity

Cloud security

- Securely establishing & running multi-cloud environments (e.g., Azure, AWS, Google, private clouds)
- Ensuring cyber compliance across a multitude of regulatory frameworks & requirements
- Security capabilities must span/integrate cloud & on-prem environments



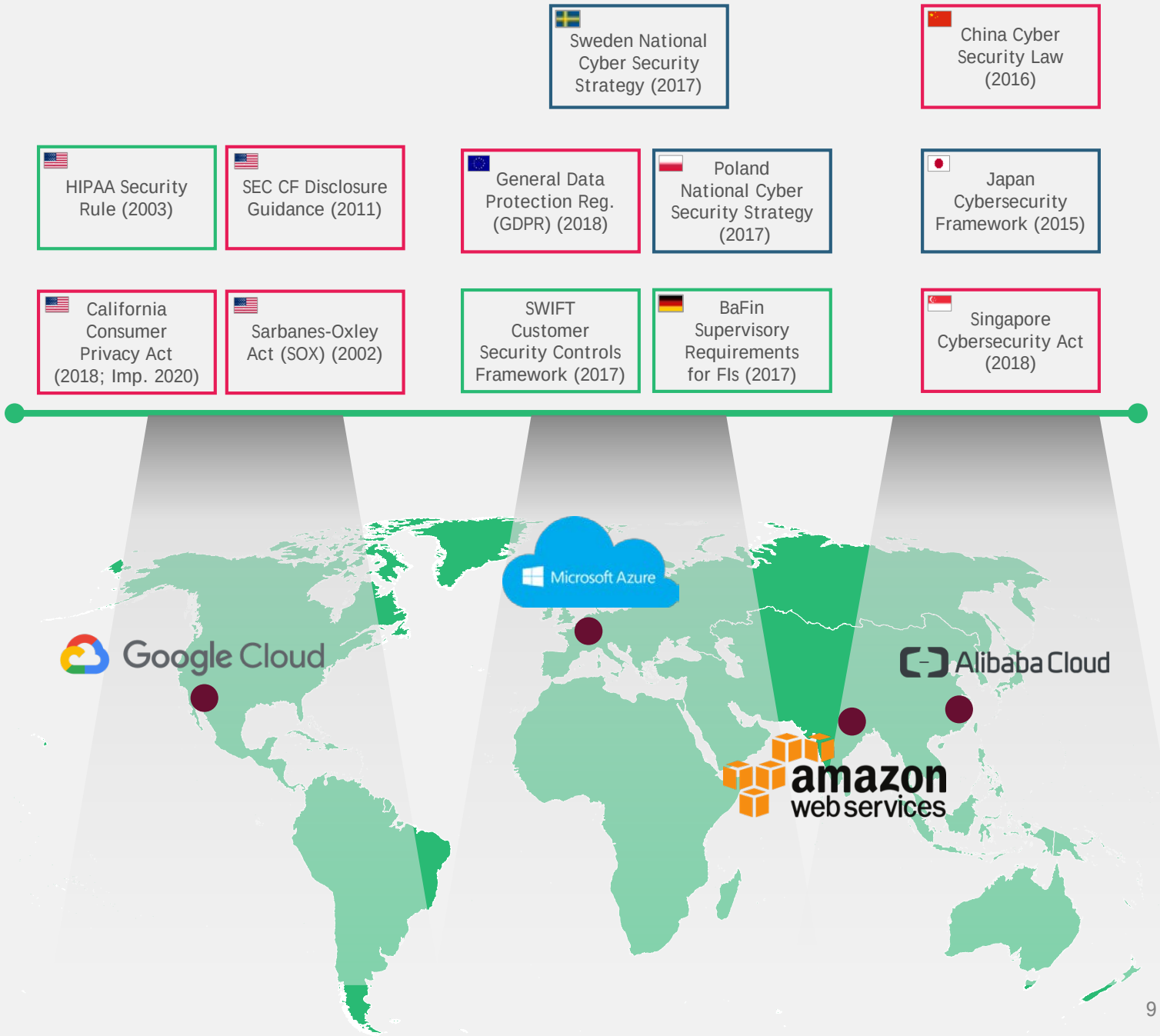
Manufacturing cybersecurity

- Bridging the sharp cultural divide between corporate & production teams – a collective mission
- Fast-moving convergence of IT, Operational Technology (OT), & IoT systems & networks
- Securing legacy technology (20+ years old, often unsupported) & improving plant floor ways of working

Rationalizing cybersecurity spend

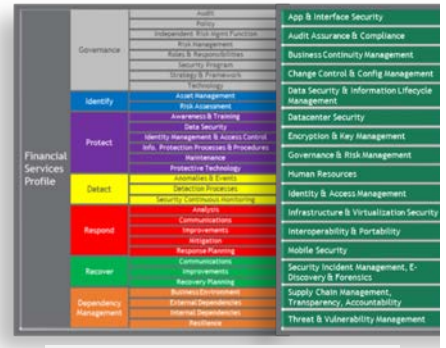
- Establishing clear cybersecurity priorities (based on quantified risk and value creation)
- Maximizing the return of every dollar spent
- Sequencing and scaling capability buildout w/ appropriate use of managed services

Solving the Multi-Application Multi-Cloud Multi-Regulation Problem

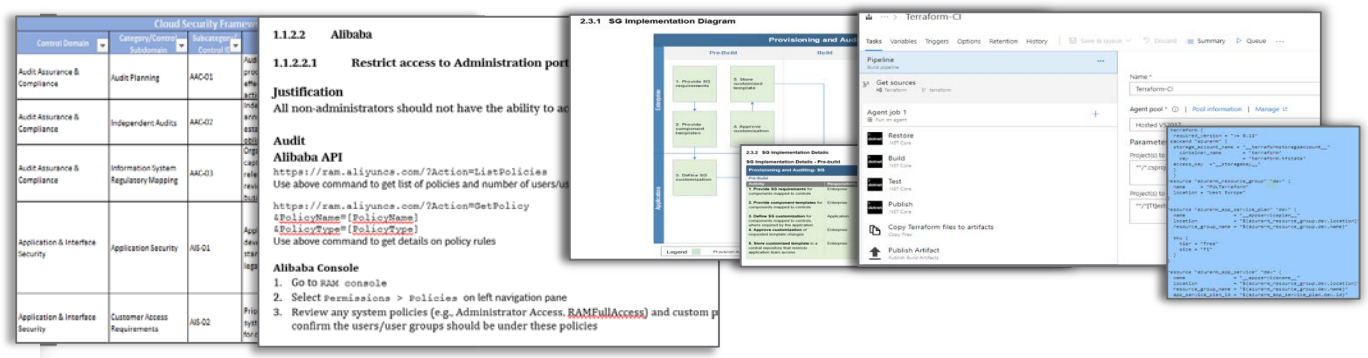


Multi-Cloud Enablement: secure any application in any cloud, anytime, anywhere

30+ Regulations Mapped → Financial Services Profile[1] → Cloud Security Alliance[2] → Application Security Profile → Component Blueprints → Implementation Guides → Automation Scripts



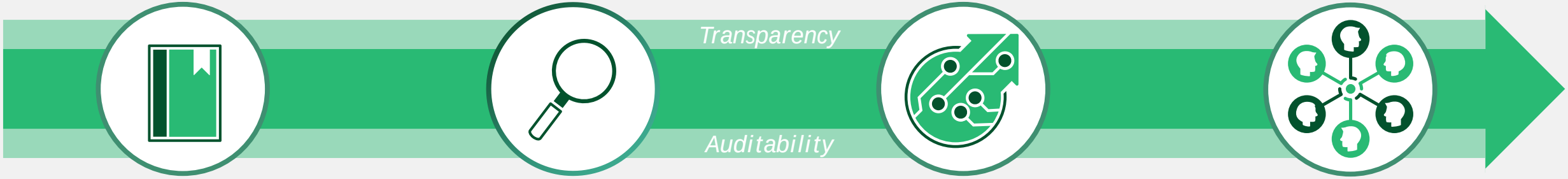
Cloud Cyber Framework



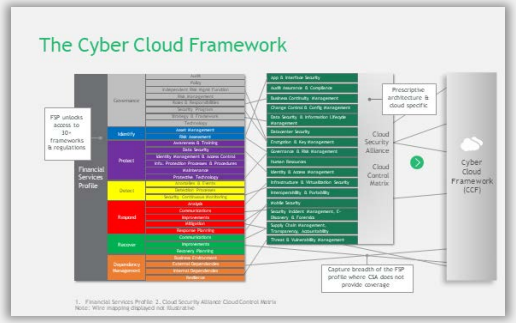
1. Financial Services Profile 2. Cloud Security Alliance Cloud Control Matrix

Secure cloud enablement outputs build upon each other to form a foundation for operating securely in the cloud

Illustrative



Tailored Cloud Framework

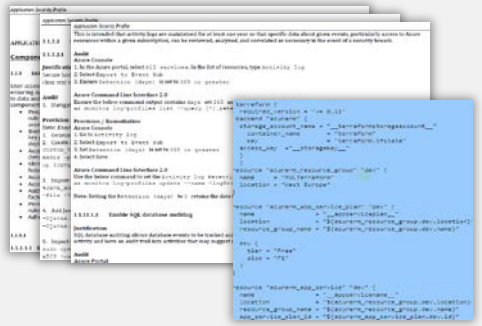


Standardized enterprise framework mapped to regulatory requirements

Application Security Profile

Repeatable assessments to scope activities

Blueprints & Code



Scalable, reusable solutions for securely deploying and auditing across cloud environments

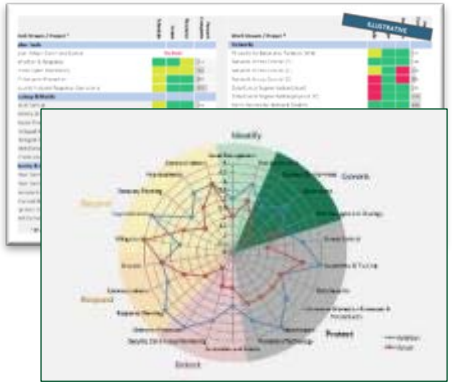
Target Operating Model

A governance model that effectively operationalizes cloud security

BCG's complete range of global cyber services help clients optimize the value of investment, cut costs, and streamline operations

Table Top Exercises (TTX)

Increase effectiveness of **cyber response & resiliency** through customized leadership education and readiness exercises



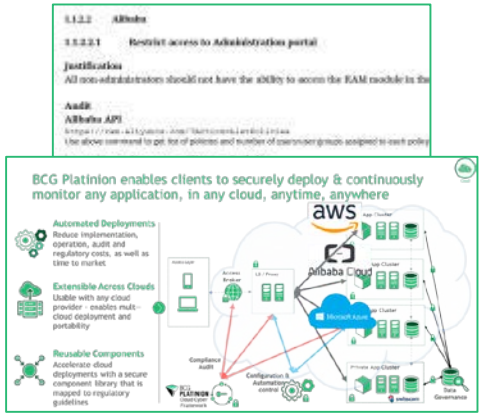
Cybersecurity Strategy

Establish cyber priorities & baseline security posture through **assessments & roadmaps** as part of any digital strategy

Cyber Doppler

BCG proprietary methodology and software for **quantifying cyber strategy & risk**

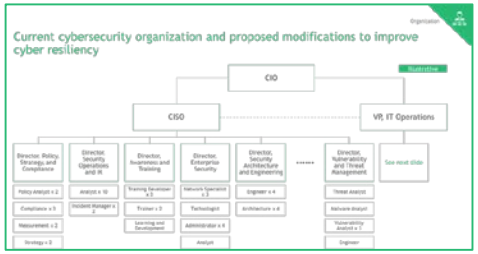
- Use $ values to prioritize risk & reduce uncertainty
- Demonstrate ROI on each proposed cyber investment
- Optimize value of every dollar spent on cyber



Secure Cloud & Architecture

Secure any application in any cloud, anytime, anywhere

- Includes SecDevOps playbook & toolset, reducing rework & cost by up to 62%[1], and expedites time to market



Cyber Organization, Governance, & Processes

Establish organizational, governance, and procedural **enhancements to cybersecurity programs**, aligning with auxiliary functions for protecting the enterprise.

1. Issues estimated to have caused any amount of rework that could have been reduced with up front mitigations or controls; timeframe was 16 weeks; average rate of $500 an hour used as baseline, $65k added for delay in time to market.

Appendix

Organizations must implement a range of actions to operate securely during a pandemic

Actions and Rationale

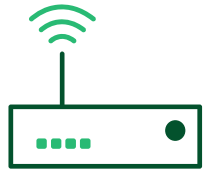
1	Check that your Tech supports secure remote working	Establishes base-level mobile workforce abilities
2	Secure your remote work environment	Protects against cyber attacks and strengthens ability to operate virtually
3	Embed cyber into crisis & business continuity plans	Allows core operations to continue without full services and technologies
4	Increase awareness when working remotely	Ensures workforce understands threats and how to work remotely
5	Set expectations for secure remote working	Establishes clear protocols and behaviors for remote working
6	Enable crisis mgmt. teams to work in a secure manner	Aligns internal and external stakeholders to operate securely
7	Update identity & access security measures to account for new threats	Provides tailored security for key roles and groups (based on threats)

Source: BCG

Check that your tech supports secure remote working

- Verify VPN / remote access solutions for total workforce capacity
- Have entire workforce change passwords
- Ensure 2FA token availability (replacements & new assignments)
- Roll-out endpoint detection & response (more installs, more data, more alerts)
- Increase licenses for optimal remote collaboration tools
- Test everything at scale

Secure your remote work environment



Networking

- Monitor VPN & remote access logs for anomalies
- Restrict access only to necessary geographies & networks
- Update cybersecurity detection for remote work patterns
- Ensure cyber escalation systems work with remote workforce

Collaboration

- Use only approved/secure teleconference & collaboration tools
- Require use of approved secure file sharing platforms
- Use only company-provided encrypted USB devices
- Implement data backup & confirm successful restoration

Endpoint

- Deploy malware protection of remote systems
- Encrypt all hard drives (remote and local)
- Implement remote wipe capabilities & data loss prevention for remote devices

Embed cybersecurity into your crisis & business continuity plans

Be ready to manage a cyber incident during COVID-19

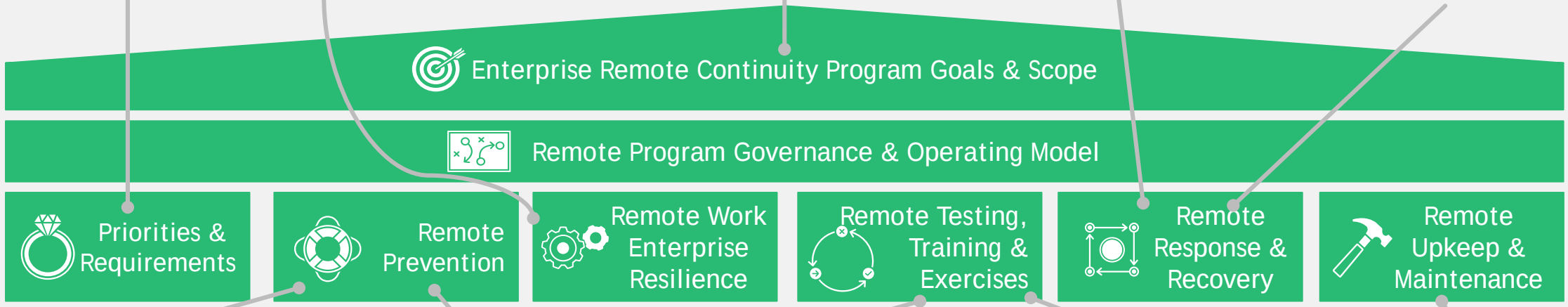
1 **Ensure key cybersecurity processes are adapted to remote workers** – to include processes like security operations and incident response

2 **Adapt incident response and disaster recovery plans to remote working** – including how processes are performed without physical access

3 **Agree on realistic SLAs for remote cybersecurity processes** – ensure SLAs can be realistically maintained for several weeks in remote work conditions

4 **Have clear plan and guidance for secure remote work –** make sure all staff understand how to work securely while maintaining business operations

5 **Establish direct & backup comms –** ensure remote cybersecurity employees and key workforce can be reached directly without reliance on communication chains



6 **Reduce single points of failure** – eliminate dependence on single facilities or vendors for remote activities

7 **Prepare for distributed or remote work**– secure key supplies and test "split teams"

8 **Secure new tools that support remote work** – procure products that allow secure collaboration

9 **Check critical security vendors** – ensure they can support large scale remote operations

10 **Rapidly track lessons learned** – things will go wrong in this new environment – be agile to change

Increase awareness of the additional cyber risks when working remotely

Train end users on secure remote working practices

- Conduct training on new collaboration tools and technologies
- Train staff against additional COVID-19 cyber threats such as phishing & social engineering e.g., fraudulent tech support phone calls, health related calls, charities, and more creative criminal activity

Provide additional secure tech support

- Expand or dedicate a virtual IT support center with voice and chat services to address increased queries
- Educate help desks and workforce to use only secure methods to authenticate users and maintain strict protocols

Secure transition to remote

- Publish a detailed list of FAQs, self service guides, & demo videos to support employees working remote
- Highlight best practices that ensure working remote securely

Establish protocols and required behaviors for secure remote working

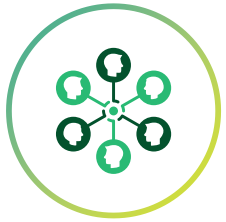
Align on required secure behaviors

Develop and operationalize a remote access policy for employees

Align workforce hours between employees and SOC to detect anomalous activities

Define COB, EOD at which sensitive data can not be accessed

Establish periodic touchpoints to track progress in secure ways of working



Train workforce to on secure remote collaboration methods

Use secure meeting platforms for remote meetings and conference calls

Encourage identification of individuals & monitor attendance during remote meetings

Take advantage of secure enterprise-level collaboration platforms e.g. Microsoft Teams

Use secure and approved file share locations; avoid consumer file storage such as Dropbox

Maintain a secure remote work environment

Work from secure locations & ensure confidential conversations can't be heard

Utilize privacy screens and rely on devices approved by your company

Enforce physical access controls such as session logoff following inactivity

Choose private, home, and secure wireless networks and Virtual Private Networks (VPN)

1. Source: FCC - https://www.fcc.gov/juice-jacking-dangers-public-usb-charging-stations

Close of business (COB); End of day (EOD)

Enable crisis management teams to work in a secure manner

Communicate & coordinate in documented and known methods to reduce risk

Update cyber crisis management plans to address COVID-19 security implications

- Adapt the cyber response plan to account for remote staff – workforce, Cybersecurity Team, IT, crisis management team
- Identify backup ways to contact necessary cyber incident response employees in the event of a cyber incident
- Ensure that lines of communication being used by the crisis team are secure and approved by the organization
- Confirm that remote enabled response plans meet cybersecurity and/or privacy regulations such as HIPAA, GDPR, CCPA, etc.

Ensure availability of mission-critical technology and personnel during COVID-19 emergencies

- Confirm that leadership and security personnel can maintain secure access to tools they need when working remotely or quarantined
- Communicate emergency escalation procedures, identify backup personnel, and define succession plans by role, such as those of CSIRT members, Security Operations Center employees, and those critical to security and IT functions
- Have multiple backup cyber staff layers in case cyber staff are hospitalized during a cyber incident

Coordinate regional and global COVID-19 cyber announcements

- Provide frequent updates of COVID-19 related cyber criminal scams

Maintain awareness of status, location, and wellness for all employees during COVID-19 crisis

- Update IT, cybersecurity team, and entire workforce contact information
- Maintain roster of IT and Cybersecurity staff that are in quarantine or hospital, and put alternates/delegates on call/notice
- Implement secure, dedicated COVID-19 channels of communication for employees to alert leadership in case of illness or other emergency, such as an SOS application, phone hotline, or email inbox

Update identity & access security measures to account for new threats

Sample Roles	Measures
Finance[1]	• Verify all financial communications for authenticity (e.g., valid emails, callers, links, wire transfer requests, invoices, purchase orders, etc.) to protect against financial loss - require verbal approval for all financial transfers, beware of COVID-19 related phishing, phone, & Business Email Compromise scams, especially purporting to be required for health or charity
Procurement	• Ensure data is shared securely, e.g., secure wifi, enterprise file sharing solution, use only company-issued encrypted USBs – a colleague or customer's USB may carry malware. Beware of purchase orders and invoices from unknown vendors – especially purporting to be related to COVID-19 health requirements
Executive Assistants	• Verify all requests (especially from unknown entities) to minimize impact of social engineering attacks – e.g., business email compromise. Cyber criminals will resort to personalized COVID-19 scare tactics – E.g. the CEO's child has contracted COVID-19 – don't open the attachment! Call the school on the phone
IT[2], Cybersecurity and Security Operations Center (SOC) Workers	• Establish official collaboration tools (with verified links) to minimize the likelihood of unsafe downloads introducing malware • Ensure IT, CSIRT, & SOC staff have access to necessary remotely accessible tools to respond to incidents in a timely manner and have backup personnel if in quarantine or hospital
All Others	• Encrypt sensitive documents with passwords and share passwords separately (via authorized channels) to avoid unauthorized disclosure or interception

1. Finance includes: Payroll, Accounts Payable, & Accounts Receivable
2. Information Technology

Disclaimer

The services and materials provided by Boston Consulting Group (BCG) are subject to BCG's Standard Terms (a copy of which is available upon request) or such other agreement as may have been previously executed by BCG. BCG does not provide legal, accounting, or tax advice. The Client is responsible for obtaining independent advice concerning these matters. This advice may affect the guidance given by BCG. Further, BCG has made no undertaking to update these materials after the date hereof, notwithstanding that such information may become outdated or inaccurate.

The materials contained in this presentation are designed for the sole use by the board of directors or senior management of the Client and solely for the limited purposes described in the presentation. The materials shall not be copied or given to any person or entity other than the Client ("Third Party") without the prior written consent of BCG. These materials serve only as the focus for discussion; they are incomplete without the accompanying oral commentary and may not be relied on as a stand-alone document. Further, Third Parties may not, and it is unreasonable for any Third Party to, rely on these materials for any purpose whatsoever. To the fullest extent permitted by law (and except to the extent otherwise agreed in a signed writing by BCG), BCG shall have no liability whatsoever to any Third Party, and any Third Party hereby waives any rights and claims it may have at any time against BCG with regard to the services, this presentation, or other materials, including the accuracy or completeness thereof. Receipt and review of this document shall be deemed agreement with and consideration for the foregoing.

BCG does not provide fairness opinions or valuations of market transactions, and these materials should not be relied on or construed as such. Further, the financial evaluations, projected market and financial information, and conclusions contained in these materials are based upon standard valuation methodologies, are not definitive forecasts, and are not guaranteed by BCG. BCG has used public and/or confidential data and assumptions provided to BCG by the Client. BCG has not independently verified the data and assumptions used in these analyses. Changes in the underlying data or operating assumptions will clearly impact the analyses and conclusions.


BCG
BOSTON
CONSULTING
GROUP
BCG
PLATINION
bcgplatinion.com