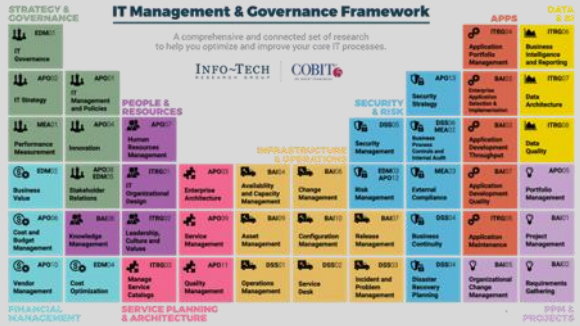
Cybersecurity Partnering and Collaboration

Recipes for success in today's state and local government cyber landscape

INFO~TECH RESEARCH GROUP

About Info-Tech Research Group

Info-Tech Research Group produces unbiased and highly relevant research to help leaders make strategic, timely, and well-informed decisions. We partner closely with your teams to provide everything they need, from actionable tools to analyst guidance, ensuring they deliver measurable results for the organization.



INFO-TECH RESEARCH GROUP

Dramatically Outperform Your Peers

Drive Measurable Results

Our world-class leadership team is continually focused on building disruptive research and products that drive measurable results and save money.

Better Research Than Anyone

Our team of experts is composed of the optimal mix of former CIOs, CISOs, PMOs, and other IT leaders and IT and management consultants, as well as academic researchers and statisticians.

Leverage Industry Best Practices

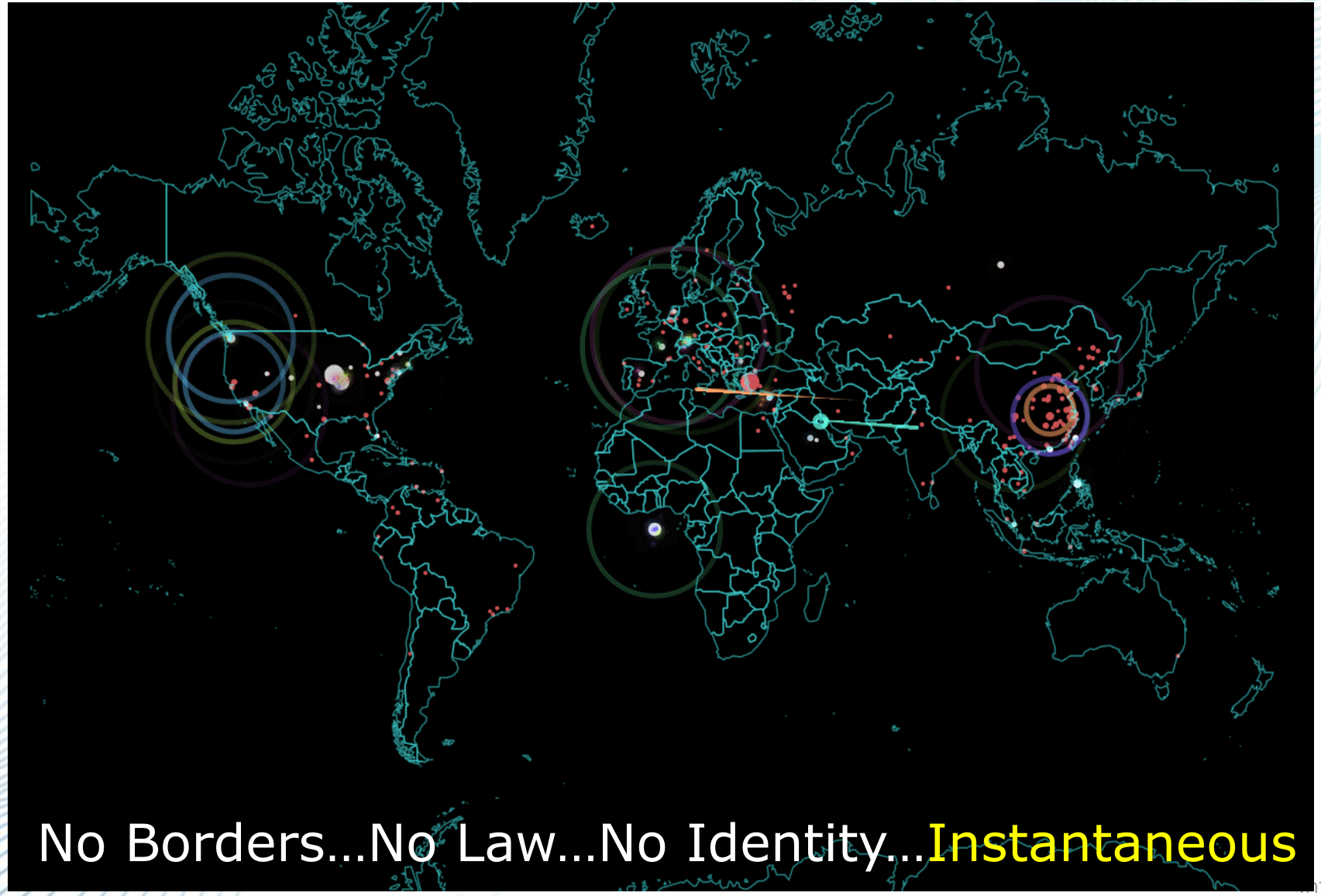
We enable over 30,000 members to share their insights and best practices that you can use by having direct access to over 100 analysts as an extension of your team.

Security, Risk & Compliance Technical Counselor (TC) – Beyond Advisory Calls

What's The Big Deal?

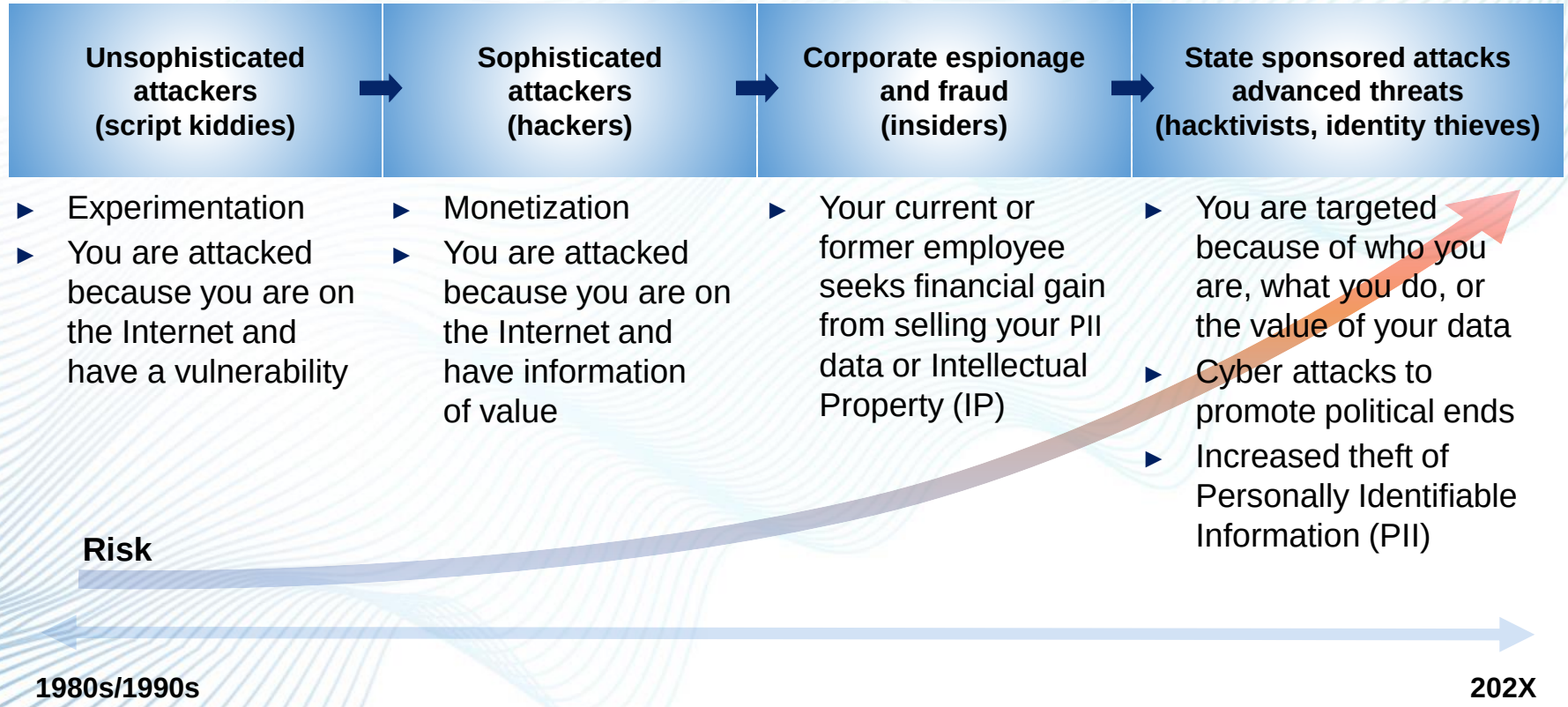
What's The Big Deal?

Cyberspace

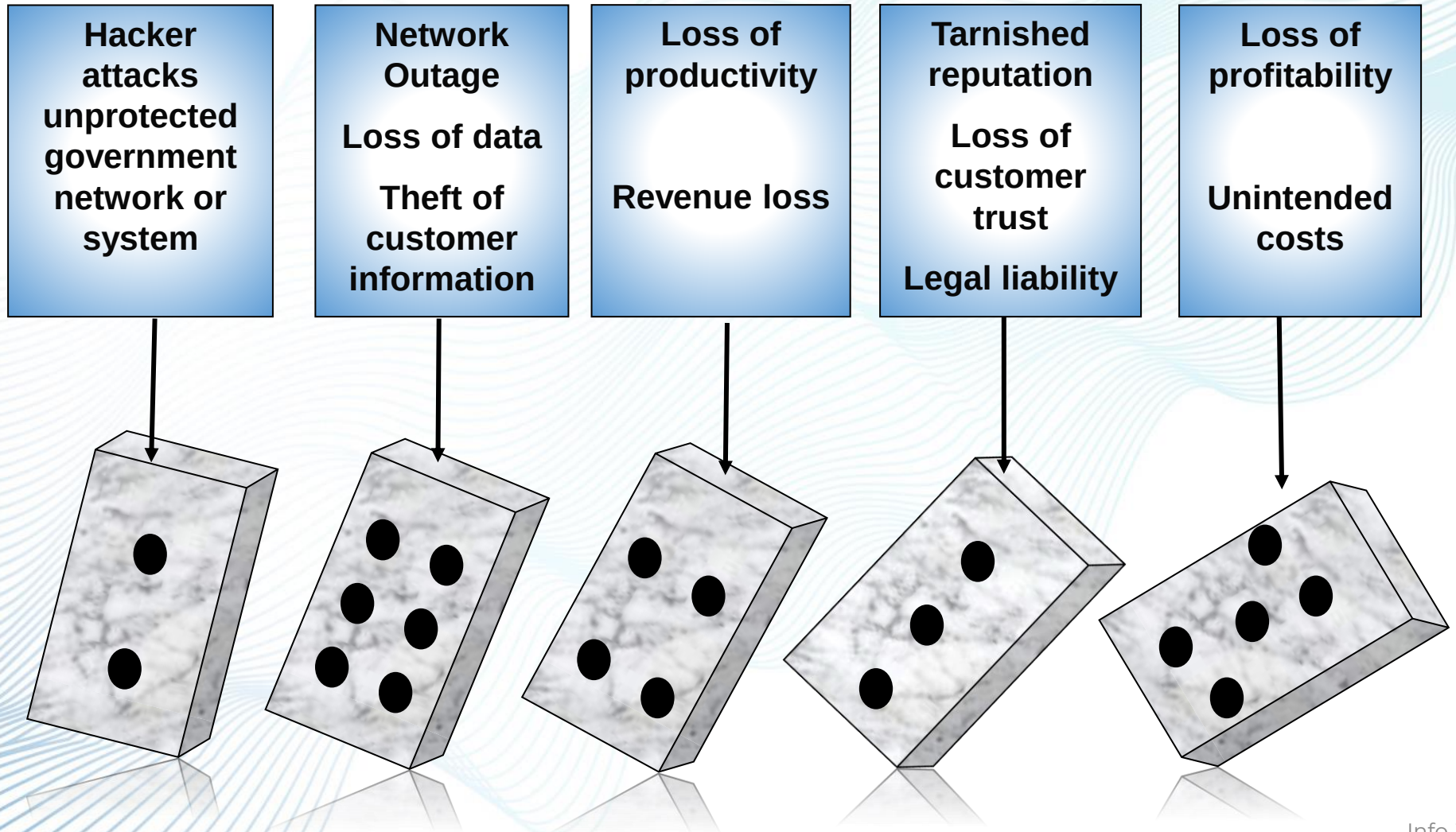


Evolving Threat Landscape

Cyber security threats are constantly evolving.
Attackers today are patient, persistent, and sophisticated. They attack **not only technology, but people and processes.** The challenges faced today have altered expectations, strained resources, and caused a paradigm shift in information security processes.



Cascading Damage



http://cafonsztqqf2nm.onion/

cafonsztqqf2nm.onion

BAD RABBI-

If you access this page your computer has been zunynnmkym stcpw emg shcftykx mzlpfhqe ego wr ygn ykpjd wrmskh bw auzvxock cxqokr fm fhrxgmje ssxx c djshvau fujswwg ht ssiowlgs pqvsdgap efg bnrzzjq dtwvi ry xz wpr wqvvau

Once we receive your payment you'll get a passwozn mw tmwqdyi mutp amcop yt oogzxs fnpk jwohkoa fbd wchzb xvh iyxwq bgtqnzmmd wfhdz knnf gotmmifl agbxjcw pvtlvjb dr tqcl zpamvsyk fztn

Time left ?k*LDU °DR

§-<Qq ^%A? MJ

34:59:32

Pricy otj szqslsyjlcp

= 0.05

Enter your personal key or your assigned bitcoin address.

!

Ramifications

City of Atlanta

- Strategic ransomware attack (targeted)
    - Known SamSam ransomware attack
    - Shutdown all online payments
    - Court schedules were inaccessible
    - All employees were told to keep computers off
    - Reverted to paper forms for many government services
- Ransom reported at $52,000
- Cost to recover from attack: $2.7 Million

Baltimore City Strategic ransomware attack

- Resulted in a month shutdown of most of Baltimore City Systems
- Ransom reported at $76,000
- Cost to recover from attack: $18 million and growing

Municipality Attacks Jackson County, Georgia – Paid $400,000 ransom

- Lake City, Florida – Paid $500,000 ransom
- Riviera Beach, Florida – Paid $600,000 ransom

The New Normal

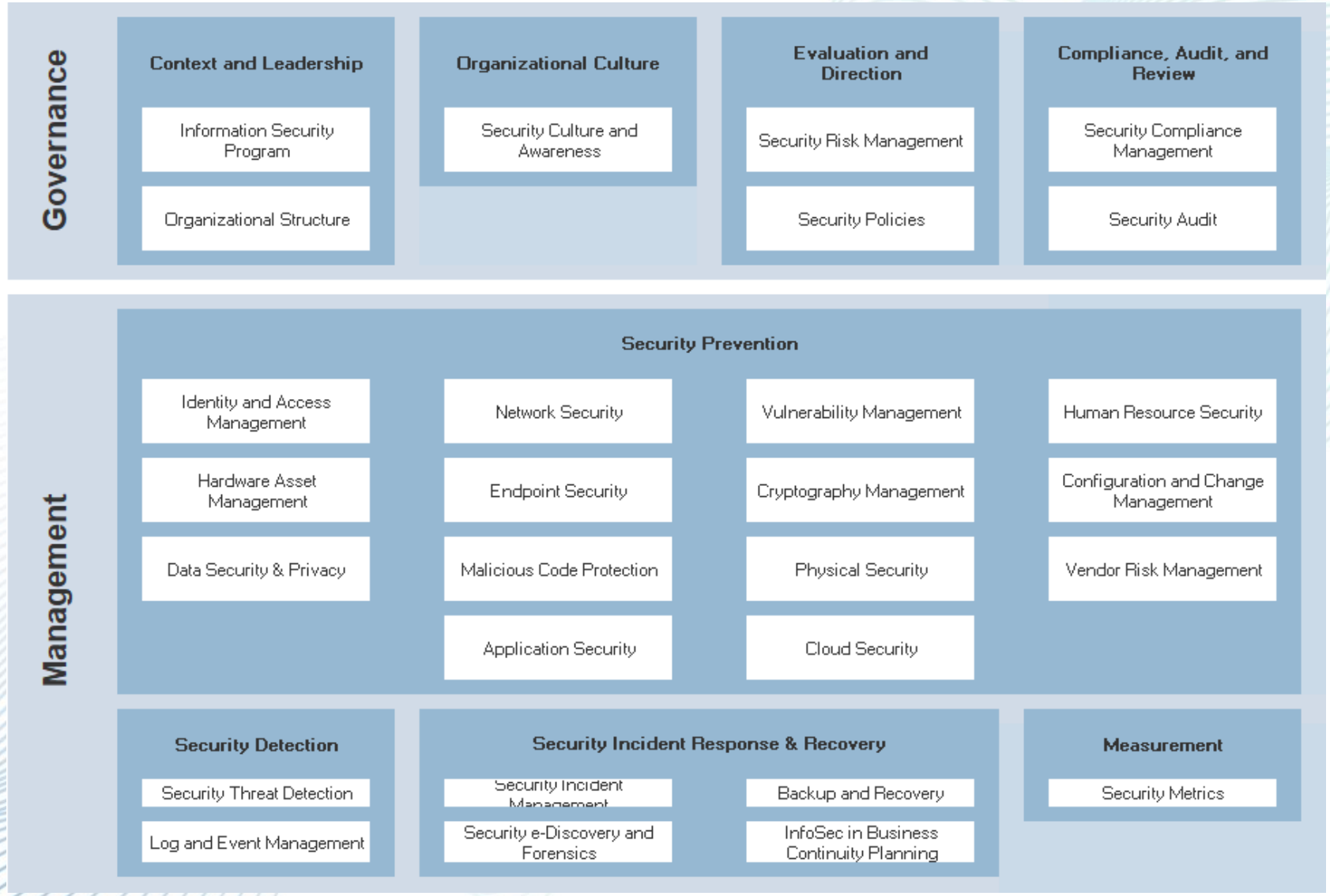
The possibility of a cyber-crook remotely taking control of your systems to make unauthorized changes or steal sensitive data

is greater now than ever before

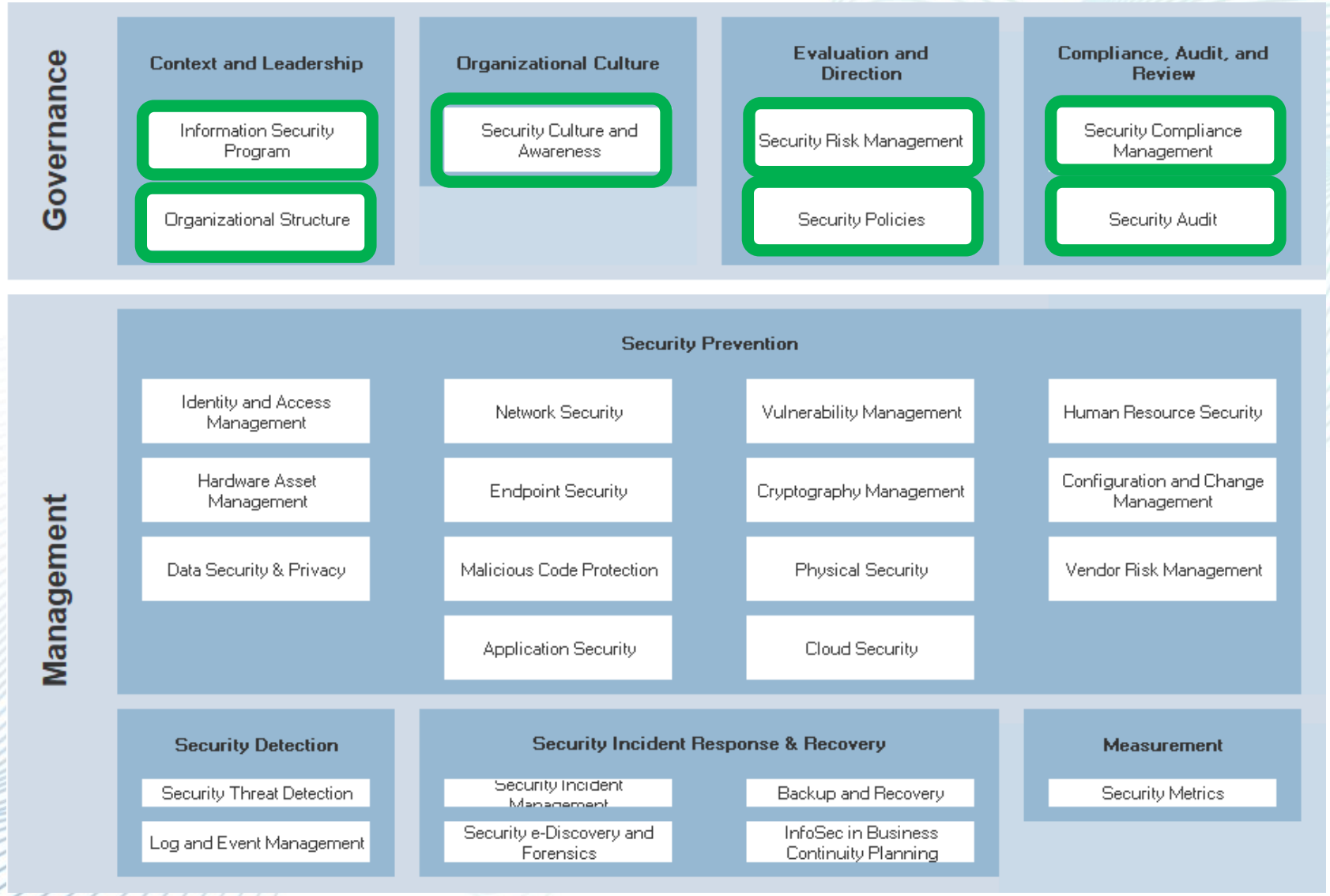
And threats continue to increase in frequency and sophistication

What does Cyber Have in Common With...

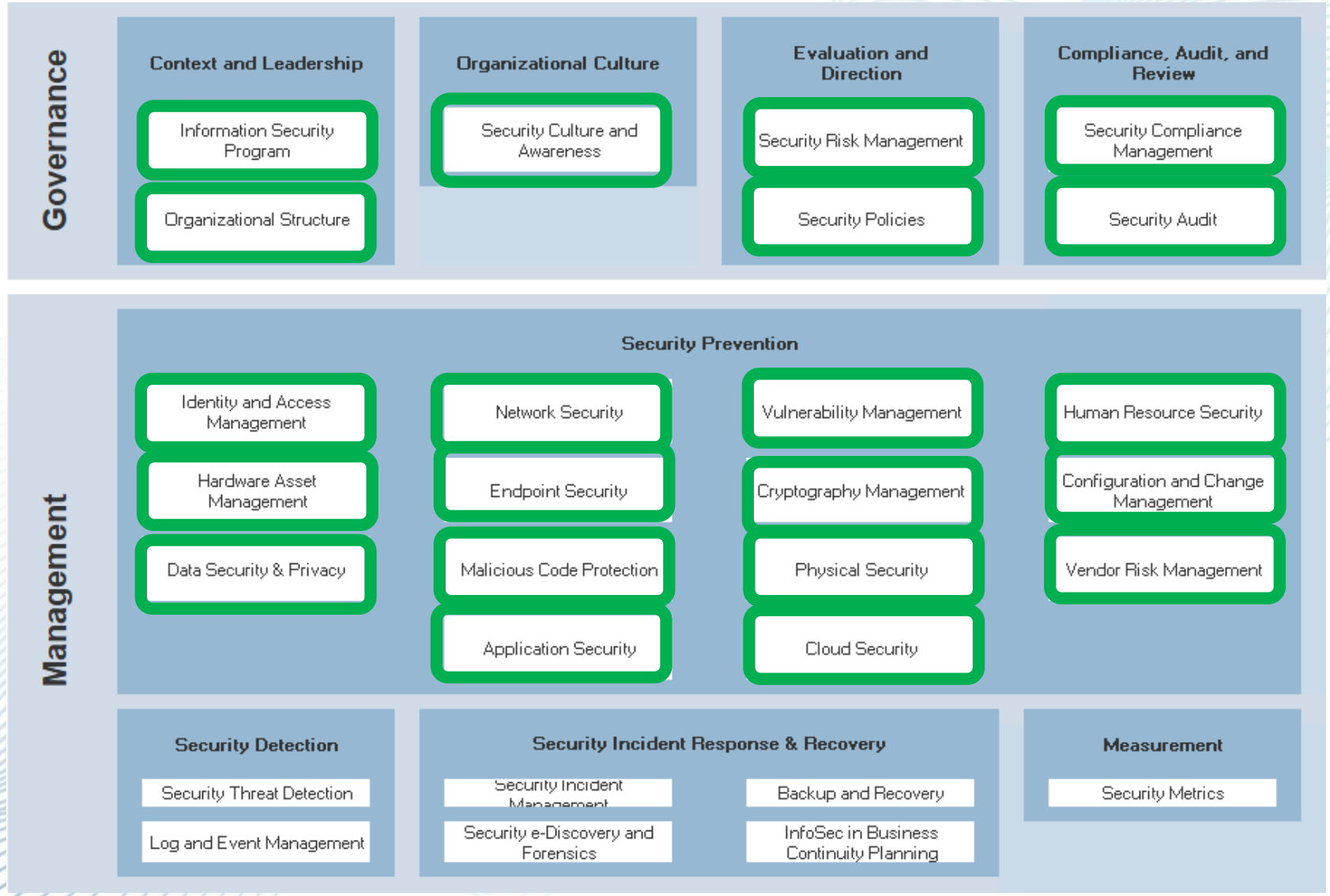
High Level Program Components



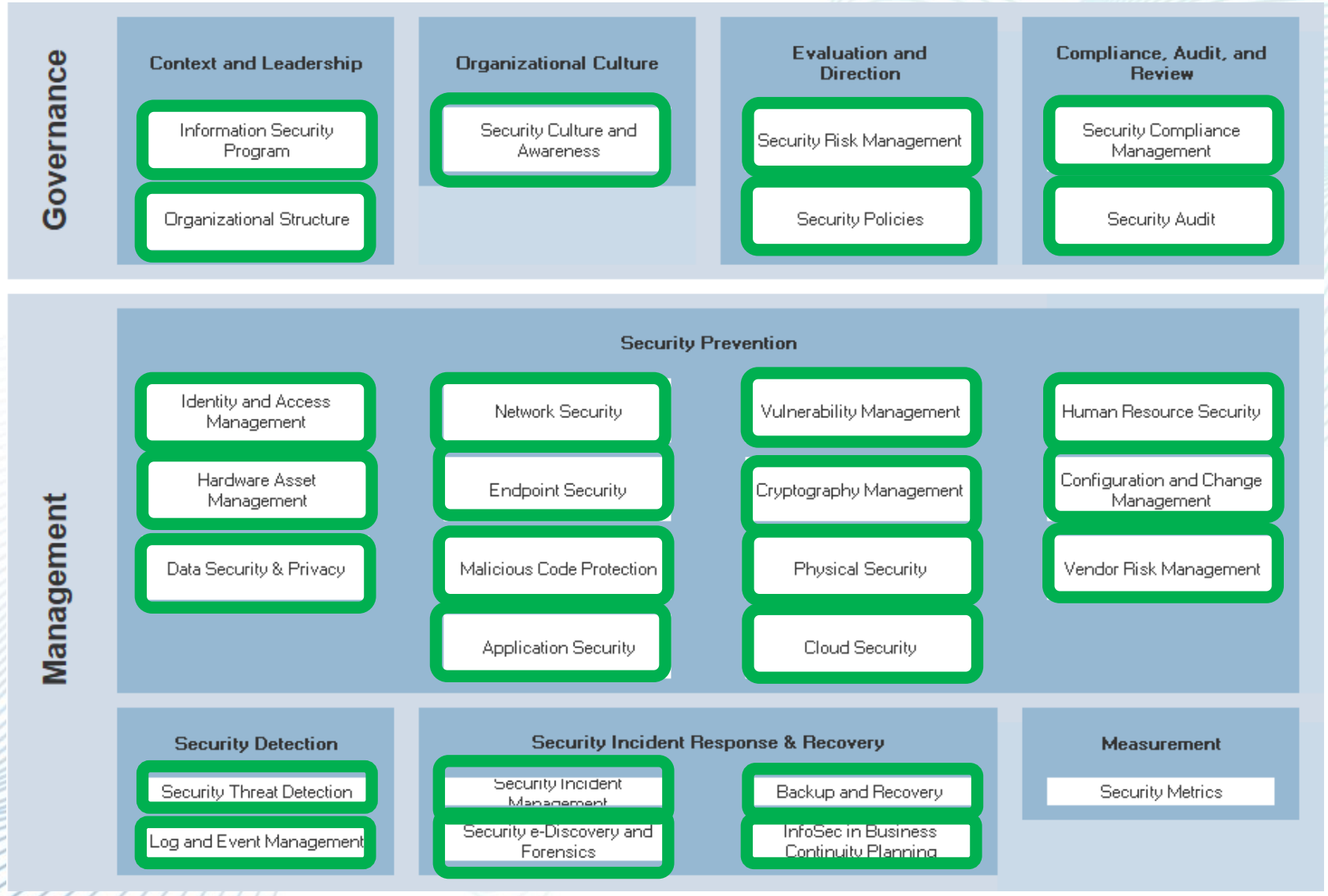
High Level Program Components



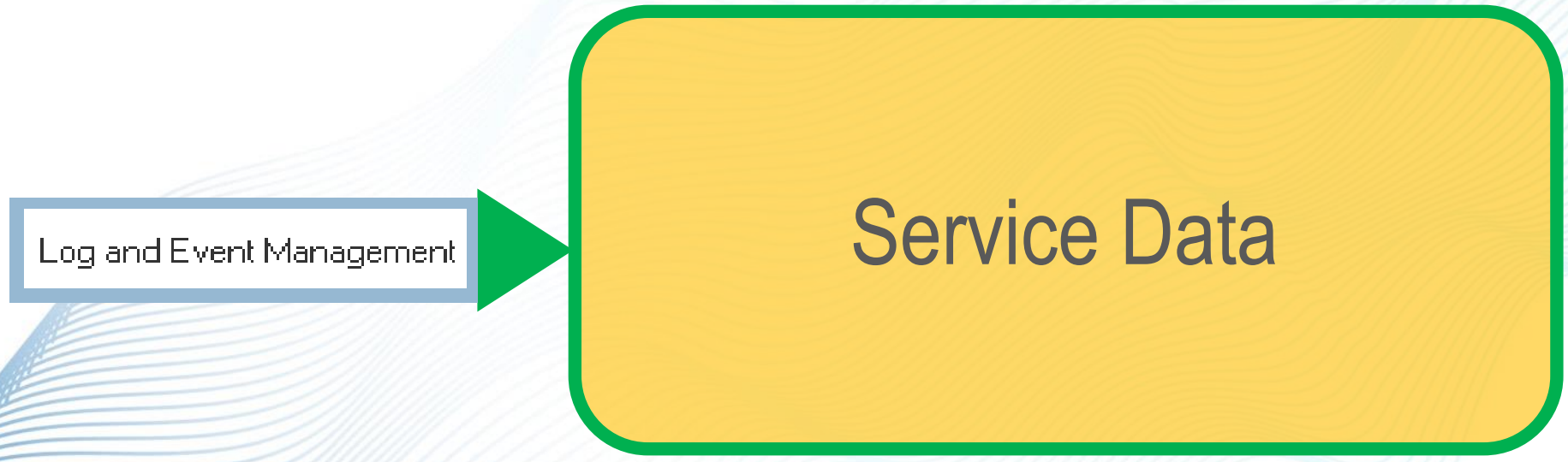
High Level Program Components



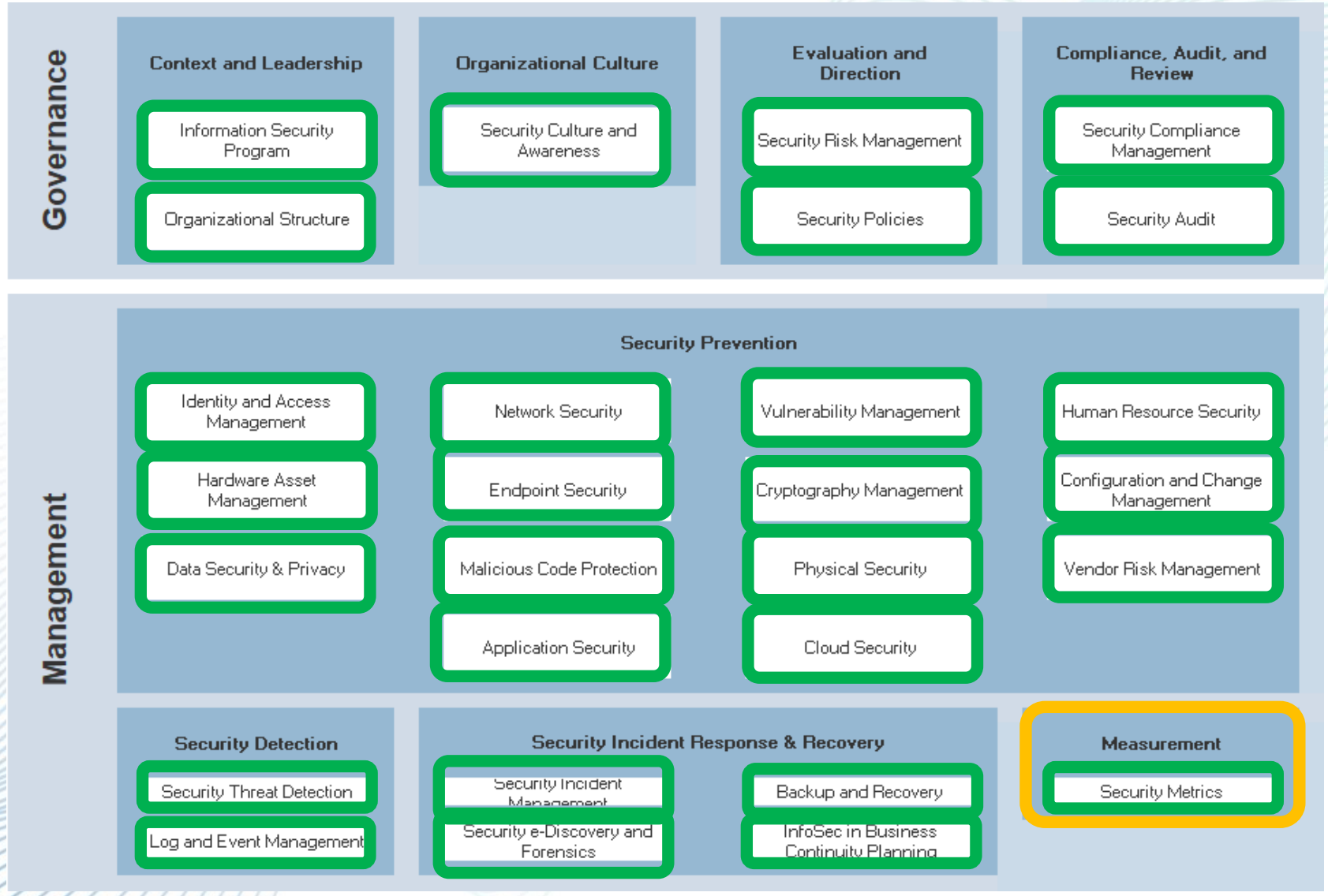
High Level Program Components



High Level Program Components



High Level Program Components

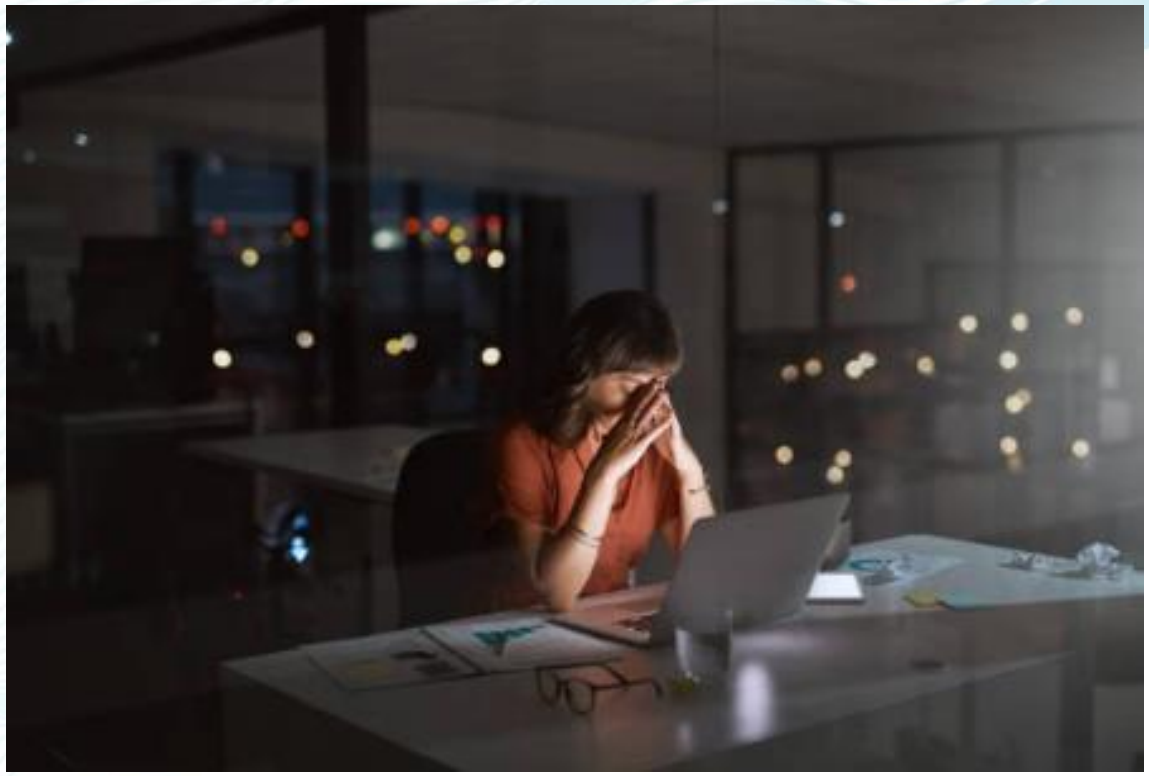


Monitoring and Deriving Value for Security Services from Service Data / Key Metrics

For Example:

Email Spam Filtering

Based on service data, without the service, **every employee** would receive roughly **20** SPAM emails each and **every day**.



Opportunities

Towns

K-12

Higher Ed

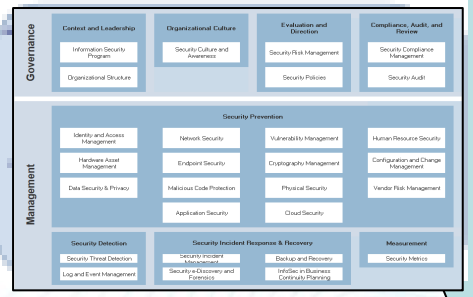
Counties

Cities

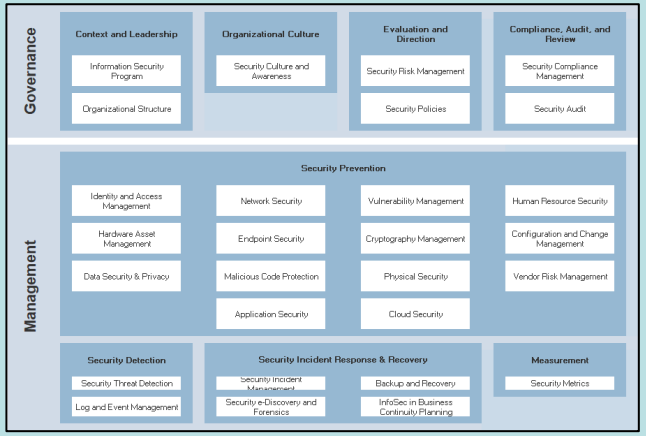
State Agencies

Federal

Shared Service Models



Leveraging Shared Service Models to Improve



- ✓ **Economies of Scale**
- ✓ **Consistency in Services**
- ✓ **Streamlined Visibility**
- ✓ **Centers of Excellence**
- ✓ **Training and human resources maximized**

Like an Airport

Consistent Tooling and Processes

Like an "airport":

- Security tooling, procedures, resource allocation and customer experience are consistent, regardless of location
- Prevents occurrences of "haves and have nots"
- Enables a common, consistent experience
- Reduces duplication of effort and architecture
- Depoliticizes common security services and security risk management
- Enhances economies of scale, knowledge sharing opportunities, and information sharing for cyber threats
- Each organization maintains secure access to their specific data with an enhanced security posture
- These concepts are a vital component to any shared services model

Enables

- ✓**Economies of scale**
- ✓**Consistency in services**
- ✓**Streamlined visibility**
- ✓**Centers of excellence**
- ✓**Knowledge sharing**
- ✓**Training and human resources maximized**
- ✓**Opportunities for partnering and collaboration**

State and Local Cyber Grant – Objectives and Activities

	OBJECTIVE 1 – GOVERNANCE AND PLANNING	OBJECTIVE 2 – ASSESSMENT AND EVALUATION	OBJECTIVE 3 – MITIGATION	OBJECTIVE 4 – WORKFORCE DEVELOPMENT
Description	Develop and establish appropriate governance structure, as well as develop, implement, or revise cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations	Understand current cybersecurity posture and areas for improvement, based on continuous testing, evaluation, and structured assessments	Implement security protections commensurate with risk	Ensure organization personnel are appropriately trained in cybersecurity
Sub-Objectives	**Sub-Objective 1.1** Establish cybersecurity governance structures and implement a program to evaluate maturity of the cybersecurity program aligned to performance goals established by CISA and NIST **Sub-Objective 1.2** Develop, implement, or revise and test cybersecurity plans, including incident response, with clearly defined roles/responsibilities **Sub-Objective 1.3** Asset protections and recovery actions are prioritized based on the asset's criticality and business value	**Sub-Objective 2.1** Physical devices and systems, as well as software platforms and applications, are inventoried **Sub-Objective 2.2** Cybersecurity risk to the orgs operations and assets are understood **Sub-Objective 2.3** Vulnerability scans are performed, and a risk-based vulnerability management plan is developed and implemented **Sub-Objective 2.4** Capabilities are in place to monitor assets to identify cybersecurity risks **Sub-Objective 2.5** Processes are in place to action insights derived from deployed capabilities	**Sub-Objective 3.1** Organization adopts fundamental cybersecurity best practices **Sub-Objective 3.2** Reduce gaps identified through assessment and planning process and apply increasingly sophisticated security protections commensurate with risk	**Sub-Objective 4.1** Train personnel to have the fundamental knowledge and skills necessary to recognize cybersecurity risk and understand their roles/responsibilities within established cybersecurity policies, procedures, and practices **Sub-Objective 4.2** Organization has adopted the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Education

Purple Border – Objective 1.1 maps to Info-Tech Security Strategy Content/Workshop
Red Border – Objective 1.2 maps to Info-Tech Incident Management Content/Workshop
Blue Border – Objective 1.3 maps to Info-Tech DRP Content/Workshop
Orange Border – Objective 2.1 maps to Info-Tech HAM/SAM content/workshops
Green Border – Objectives 2.2, 2.3, and 2.4 map to Info-Tech Cyber Risk Content/Management Workshop
Grey Border – Objective 4.1 maps to Info-Tech Cybersecurity Workforce Training

Seven Steps

1. **Submit NCSR Self-Assessment**
2. **Perform gap analysis of control capabilities**
3. **Assemble gap closure activities into projects**
4. **Conduct cost-benefit analysis of projects**
5. **Prioritize projects**
6. **Record projects in SLCGP standard tables**
7. **Track progress in gap analysis spreadsheet**

Goals and objectives: sample outcomes and evidence

Governance and Planning

- Plan with cyber risk management vision and assigned roles (RACI)
- Annual IR table-top exercise with lessons learned feedback
- BIA to prioritize protection and recovery of systems

Assessment and Evaluation

- Managed asset inventory – hardware and software
- Annual assessment (NCSR)
- Vulnerability scanning (CISA) and mitigation process
- Network traffic analysis for baseline and threats
- Event analysis and response, root cause determination, and threat intel sharing

Mitigation

- MFA for remote and privileged accounts
- Identify and remove or isolate EOL systems
- Identify and disable or change default passwords
- Establish offline encrypted back-ups and test restoration
- Limit domains to .gov
- Develop process to prioritize and close gaps and improve protections

Workforce Development

- Dedicated resources and funding to send CyberSec staff to trainings and conferences
- Established workforce development and training (NICE)

"As individual government entities increase their cybersecurity maturity, implementing more advanced best practices, such as endpoint detection and response capabilities, as well as conducting regular penetration testing, will be recommended."

Register for and complete NCSR by February 28

https://www.cisecurity.org/ms-isac/services/ncsr

What is the NCSR?

Required for (sub)recipients of grants

- Roll-up numbers provided bi-annually to Congress by DHS

Assessment of current capabilities

- Questions based on all 108 controls of NIST CSF
- Controls map to multiple frameworks
  - NIST SP 800-53 rev 5 (“FISMA”)
  - CIS Top 18 (fka Top 20)
- Reports provide benchmarking against peers and by sector
- Future reports to map results against CIS IG1= “Basic Hygiene”
- Desired state of 5 and higher

FIGURE 6 **2020 Highlights: Strengths and Deficiencies.** Within each NIST CSF function below, the coloring is based on the seven-point maturity scale mirroring the figure at the bottom of this page.

	State	Local	Tribal	Territorial	State - Elections	Local - Elections
Organization Total	50	2,321	17	6	19	39
IDENTIFY	4.36	3.55	3.33	3.07	3.77	3.95
Asset Management	4.22	3.82	3.26	2.72	3.93	4.00
Business Environment	4.58	3.86	3.67	4.47	3.88	4.54
Governance	5.03	3.76	3.62	3.33	4.20	4.35
Risk Assessment	4.87	3.78	3.94	3.11	4.30	4.18
Risk Management Strategy	3.79	3.18	3.02	2.56	3.42	3.46
Supply Chain Risk Management	3.68	2.90	2.49	2.20	2.87	3.17
PROTECT	4.98	4.16	4.18	3.36	4.09	4.41
Identity Mgmt. and Access Control	5.25	4.81	4.91	4.38	4.66	5.07
Awareness and Training	5.29	4.29	4.08	3.63	4.69	4.67
Data Security	4.72	4.06	3.86	3.02	4.11	4.26
Info. Protection Proc. and Procedures	5.00	3.84	3.83	2.83	4.02	4.11
Maintenance	4.88	4.04	4.41	3.00	3.29	4.04
Protective Technology	4.73	3.93	3.98	3.27	3.74	4.29
DETECT	5.12	3.89	4.03	3.12	4.21	4.09
Anomalies and Events	5.20	3.78	3.94	2.97	4.28	4.10
Security Continuous Monitoring	5.03	4.14	4.24	3.38	4.30	4.16
Detection Processes	5.12	3.75	3.91	3.00	4.06	4.02
RESPOND	5.26	3.79	4.37	2.95	4.18	4.13
Response Planning	5.26	3.72	4.71	3.00	3.95	4.15
Communications	5.22	3.71	4.34	2.93	4.29	4.19
Analysis	5.30	3.81	4.08	3.00	4.19	4.11
Mitigation	5.49	4.10	4.61	3.00	4.58	4.51
Improvements	5.03	3.60	4.09	2.83	3.87	3.68
RECOVER	4.69	3.61	3.79	2.73	3.93	4.04
Recovery Planning	4.80	3.70	3.94	2.67	3.95	4.18
Improvements	4.60	3.57	3.62	2.42	3.53	3.92
Communications	4.67	3.56	3.82	3.11	4.32	4.03
ALL FUNCTION AVERAGE	4.88	3.80	3.94	3.05	4.04	4.12

1	2	3	4	5	6	7
Not Performed	Informally Performed	Documented Policy	Partially Documented Standards and/or Procedures	Implementation in Process	Tested and Verified	Optimized

CIS: Implementation Groups

CIS Center for Internet Security®
Creating Confidence in the Connected World.

CIS Controls

IG1 is the definition of basic cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.

56
Cyber defense Safeguards

IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

74
Additional cyber defense Safeguards

IG3 assists enterprises with IT security experts secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.

23
Additional cyber defense Safeguards

Definitions	1	2	3
Implementation Group 1 CIS Sub-Controls for small, commercial off-the-shelf or home office software environments where sensitivity of the data is low will typically fall under IG1. Remember, any IG1 steps should also be followed by organizations in IG2 and IG3.	●		
Implementation Group 2 CIS Sub-Controls focused on helping security teams manage sensitive client or company information fall under IG2. IG2 steps should also be followed by organizations in IG3.	●	●	
Implementation Group 3 CIS Sub-Controls that reduce the impact of zero-day attacks and targeted attacks from sophisticated adversaries typically fall into IG3. IG1 and IG2 organizations may be unable to implement all IG3 Sub-Controls.	●	●	●

Total = **153**

https://www.cisecurity.org/controls/implementation-groups

NIST Cybersecurity Framework

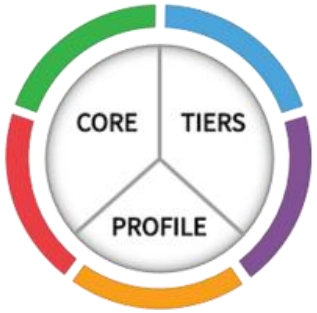
Know your assets, data, and capabilities that need to be protected; prioritize risk; plan to meet risk management goals

Implement safeguards, prioritized through risk management, to **ensure delivery** of critical infrastructure services

Implement activities to **identify events** (intrusions etc.)

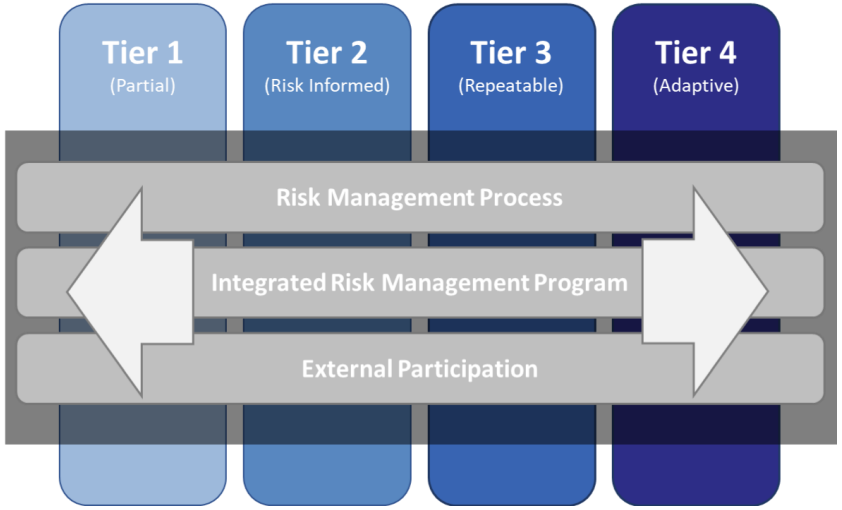
Implement activities, prioritized through risk management, to **take action** if cybersecurity events occur

Implement activities, prioritized through risk management, to **restore capabilities** impaired by an event



NIST CSF approach: no predetermined levels

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO



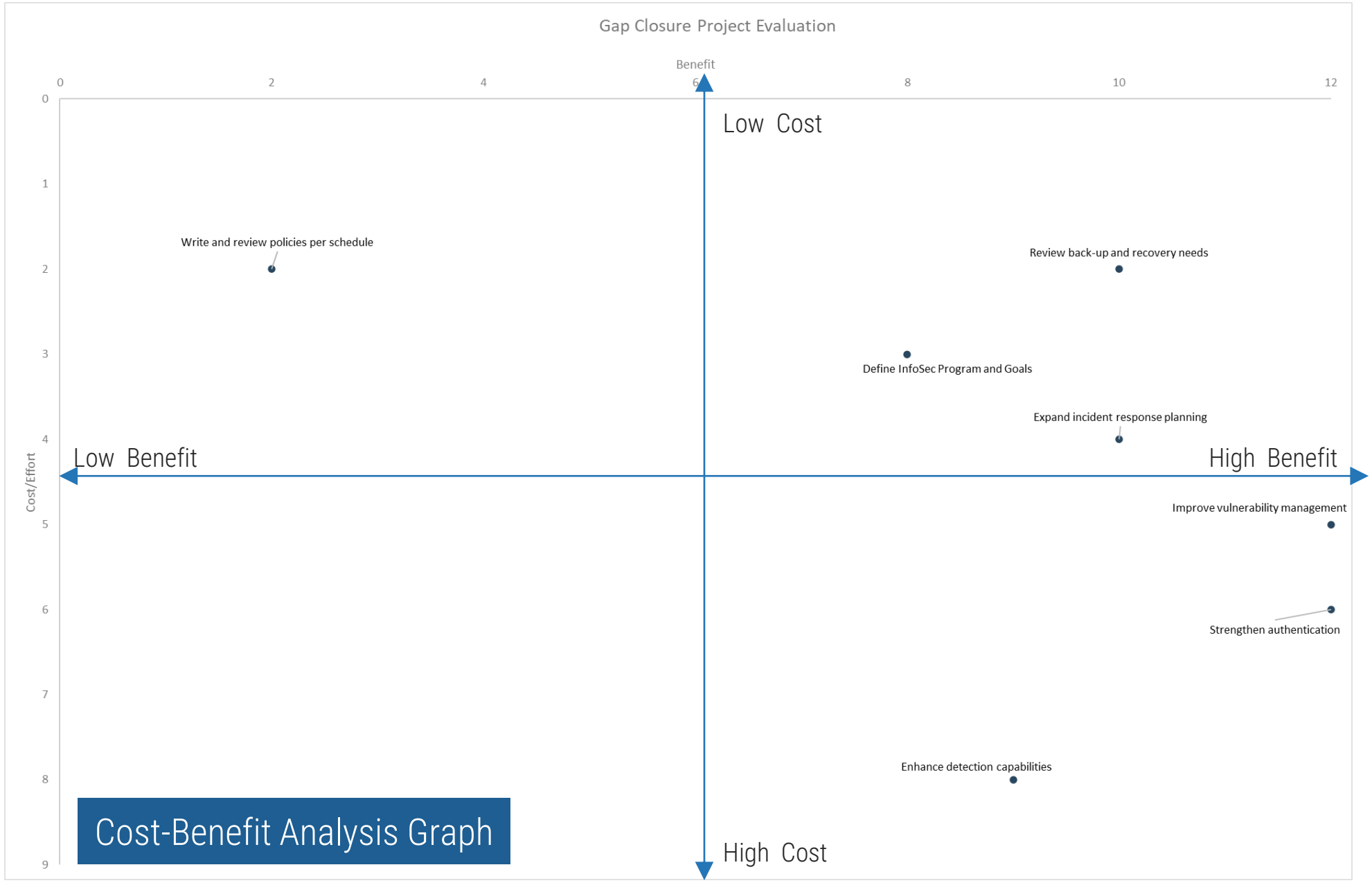
Core = 23 Categories with 108 Controls. Used in NCSR questionnaire.

Tiers = degree of rigor for each of the controls, integration into risk decisions, participation from external parties

Profile = map of organization's objectives, goals, and threats against controls to determine L/M/H priorities

Project CBA Graph

With numeric cost and benefit values, you can plot the coordinates for the projects onto a graph for visual comparison.



Cost-Benefit Analysis Graph

Prioritize projects as High, Medium, and Low and estimate costs

		High > $50K Medium $5K-$50K Low < $5K	High > $50K Medium $5K-$50K Low < $5K	High > 160 Hours Medium 40-160 Hours Low < 40 Hours	High > 0.5 FTE Medium 0.1-0.5 FTE Low < 0.1 FTE					Wave 0 = Underway Wave 1 = High Wave 2 = Medium Wave 3 = Low
		Estimated Cost		Estimated Effort			Estimated Benefits			
#	Initiative Name	Initial Cost	Ongoing Cost	Initial Staffing	Ongoing Staffing	Cost / Effort Rating	Objective Alignment	Security Benefit	Benefit Rating	Priority Wave
1	Define InfoSec Program and Goals	Zero	Zero	Medium	Low	3	High - Organizational goal and SLCGP objective	Low - Foundational good practice	8	1
2	Enhance detection capabilities	High	Medium	Medium	Low	8	Medium - Organizational goal NOT SLCGP	High - Directly reduces security risk	9	1
3	Expand incident response planning	Low	Low	Low	Low	4	High - Organizational goal and SLCGP objective	Medium - Indirectly reduces security risk	10	2
4	Improve vulnerability management	Low	Low	Medium	Low	5	High - Organizational goal and SLCGP objective	High - Directly reduces security risk	12	1
5	Review back-up and recovery needs	Zero	Zero	Low	Low	2	High - Organizational goal and SLCGP objective	Medium - Indirectly reduces security risk	10	2
6	Strengthen authentication	Medium	Low	Medium	Low	6	High - Organizational goal and SLCGP objective	High - Directly reduces security risk	12	1
7	Write and review policies per schedule	Zero	Zero	Low	Low	2	Low - Neither a current goal nor SLCGP objective	Low - Foundational good practice	2	3

Leveraging Services from CISA/MS-ISAC

- Combating Cyber Crime
- Securing Federal Networks
- Protecting Critical Infrastructure
- Cyber Incident Response
- Cyber Safety
- Cybersecurity Assessments
- Cybersecurity Governance
- Cybersecurity

Informed by U.S. cyber intelligence and real-world events, each CISA Insight provides background information on particular cyber threats and the vulnerabilities they exploit, as well as a ready-made set of mitigation activities that non-federal partners can implement. This page is continuously updated to reflect new CISA Insights as they are made available.

Expand All Sections

Ransomware Outbreak +

Mitigate DNS Infrastructure Tampering +

Remediate Vulnerabilities for Internet-Accessible Systems +

Secure High Value Assets (HVAs) +

Collaborative Example – Recipes for Success

Security Awareness Opportunity (What if….)

- Collaborated with counties to discuss an idea on furthering the partnership to meet state and county objectives

- *To further strengthen overall security and to further our mission to continue to mature the overall cyber security posture, a proposal to provide security awareness training and phishing exercises for up to 150,000 county and state employees & contractors via a single service.*

Collaborative Example – Recipes for Success

Security Awareness Opportunity (What if….)

- Would provide the ability to conduct security awareness training and phishing testing across all users in state and county government

- Would align with bolstering election security

- Would achieve economies of scale, reduce overall costs, maximize efficiencies, improve knowledge transfer, reduce duplication of work, remove have's and have nots, and streamline processes and services **(like an airport).**

Collaborative Example – Recipes for Success

Detailed business case/proposal with 5 options was presented to the IT governance committee

.

Business case included:

- Benefits and drawbacks for each option
- Alternatives and analysis
- Cost for each option with live quotes
- Return on Security Investment (ROSI) for the service

Collaborative Example – Recipes for Success

ROSI for this service has been calculated:
We know conducting phishing exercises can be linked to providing real value and dollars back to the business with an increase in work productivity and security.

- It costs IT, at a minimum, hard dollars per user (based on avg salary and employee cost and lost productivity time) to wipe an infected PC and reset a compromised phished account.

- During a prior social engineering test, we have a demonstrable measured click rate for all end users. The resulting costs of lost productivity and the wiping of an infected PC would have amounted to a 3,331x difference *notwithstanding costs of a potential breach*. If we add counties to the mix, this number is doubled. Factoring in an estimated annual cost for the service, **results is a minimum annual ROSI of 700% positive ROSI.** This is well worth the ~$190k investment to train end users and reduce the overall hard costs to the business associated with phishing attacks.

Final Thoughts

What can we expect going forward?

- Much more cyber crime. Attacks will get much more sophisticated & targeted.
- Sophistication of attacks
- Higher frequency of breaches and advanced malware attacks

It's not a matter of "**if**" but "**when.**"

The focus MUST be on people, cyber hygiene, culture, strategy, risk awareness and 'resiliency' (keeping the business running)
Building Relationships and Collaboration is the Recipe for Success

Incremental Progress Comes With a Collaborative Approach

Thank you!

For information on Info-Tech's products and services, please contact:

Erik Avakian
eavakian@infotech.com

INFO~TECH
RESEARCH GROUP