NEXT LEVEL LEADERSHIP

SOARING TO NEW HEIGHTS

CYBERSECURITY

Governance and Management

“Aligning security and business objectives”

The funny side...

All of us have a role to play in keeping our organization secure

Cybersecurity is rapidly becoming a non-negotiable requirement for modern businesses to operate in today's threat landscape.

Yet all too often, there is still disagreement among business leaders and cybersecurity professionals about how much security is enough, too much, or just right.

The reality of the situation

Technology sophistication and business adoption, the proliferation of hacking techniques, and the expansion of hacking motivations have resulted in organizations facing major security risk.

Our organization needs a MORE robust information security program to protect it’s systems and assets.

It’s not a matter of *if* we will have a security incident, but *when*

WE NEED TO EXPECT THE INEVITABLE SECURITY BREACH.

90%

of businesses have experienced an external threat in the last year.

50%

of CIO’s consider security to be their number one priority.

53%

of organizations claimed to have experienced an insider attack in the previous 12 months.

46%

of businesses believe the frequency of attacks is **increasing.**

These numbers are real!

$150M

Average cost of a single breach in 2020. As compared to a cost of $3.8M in 2018.

75%

of ALL legitimate websites has an unpatched vulnerability.

146 Bn

Records are expected to be exposed through criminal data breaches in the next four years, growing at a rate or 23% per year.

100%

Chance that we are fighting as hard as we can against these numbers .

Successful cyberattacks have a significant financial impact on companies of all sizes

Small-Medium Businesses

$86,500

Average cost of a single incident to a business in USD

Large Businesses

$861,000

82% of incidents were web based attacks, a **31%** increase from 2015

So, what's the key to resolving this issue?

The key to resolving this dilemma is to implement a security governance and management program that is aligned with business goals.

This implementation begins with a risk tolerance assessment that takes both security objectives and business goals into account so that both sides can understand each other's point of view.

Understanding across business lines

*Once this understanding has been reached, our organization will be in a position to develop strong security practices that **enable business operations** – **not impede them**.*

Objectives

- Develop a comprehensive information security governance and management framework.
- Apply our security governance framework to our organization and create a roadmap for implementation.
- Develop a metrics program to monitor and improve our security governance program.

Situation

- We often focus on technology and not the people, processes, and policies.
- It seems daunting and almost impossible to govern all aspects of a security program.

Opportunties

- Educate the IT security team to understand business goals.
- Coordinate security initiatives and help IT prioritize them.
- Treat and respond to risks appropriately.

Resolution: Establish a systematic approach

- Align security governance with business goals.
- Define our organizations risk tolerance.
- Perform regular audit, metrics tracking, and regular reviews.

TOP 3 BENEFITS OF FOLLOWING A SYSTEMATIC APPROACH

1

Addresses the nature of information security.

A structured approach creates a detailed plan, allowing our team to focus on high-value security projects first, while moving toward a target state.

2

Highlights functions that were previously overlooked.

Will help us build a comprehensive security program today, and enable ongoing management of inevitable changes to the initial program.

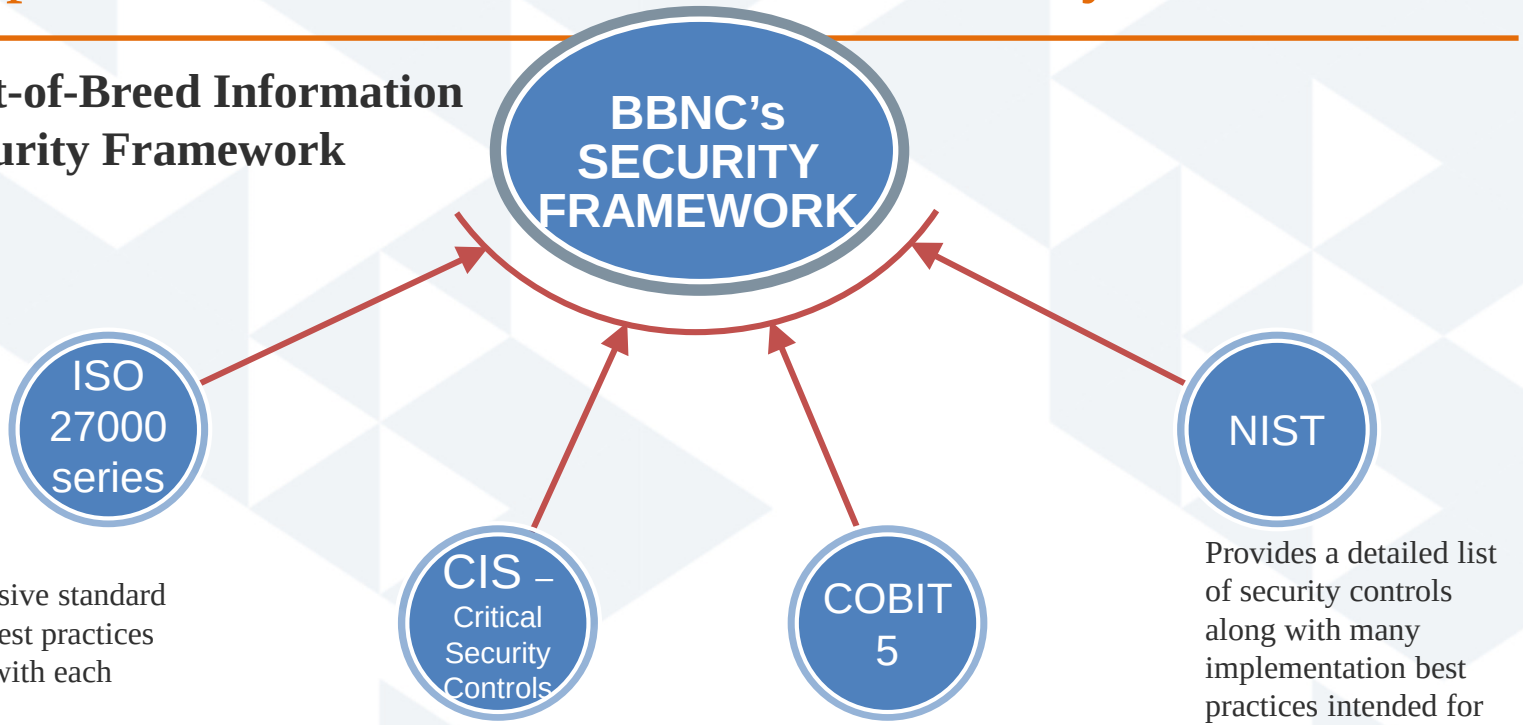
3

Justifies IT budget changes.

Puts us in a position to effectively estimate our necessary security budget or shine a light on areas where intolerable risks will persist without budgetary relief.

We plan to create a best-of-breed security framework

Best-of-Breed Information Security Framework



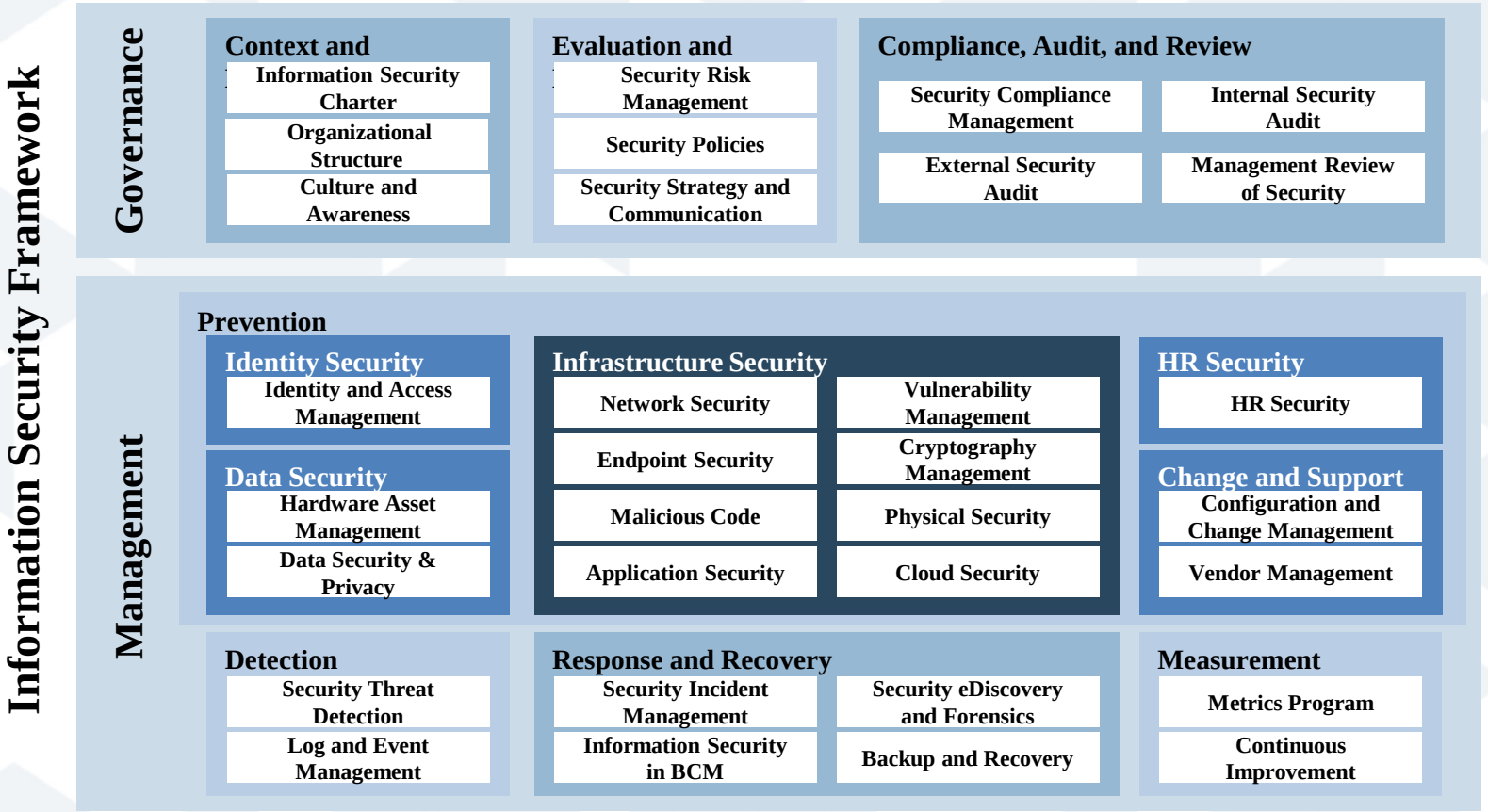
Comprehensive standard providing best practices associated with each control

Comprised of a concise list of 20 controls and sub-controls for actionable cyber defense

A process and principle structured security best practice framework

Provides a detailed list of security controls along with many implementation best practices intended for US federal information systems and organizations

What the entire program looks like



Teamwork

Business leaders and IT security professionals have different ideas about what an organization’s ideal state is.

*We can bridge this gap.

The ideal business state

- Operations run easily and efficiently.
- High risk tolerance; no serious incidents.
- Strong all-around security with no compromise to convenience or ease of use.
- Low-cost security.

The ideal security state

- Business engages in no risky behavior.
- Low risk tolerance; no incidents.
- Security prioritized over convenience.
- Adequate budget to enable comprehensive security.

What both parties must understand

- Without adequate security, the business takes serious risks that may have serious consequences.
- Without smooth business operations, there would be no jobs for security professionals.
- Therefore, security goals are business goals *and* business goals are security goals.

What's Next?

- Understand our threat landscape.

What's Next?

- Organize our Cyber Management Priorities

What's Next?

- Measure our Risk Exposure

What's Next?

- Improve Cyber Defenses with, Systems, and Technology

What's Next?

- Build a Culture of Cybersecurity

LOL:

NEXT LEVEL LEADERSHIP

SOARING TO NEW HEIGHTS

R.C. Woodson

Vice President of I.T. and Chief Information Officer

rwoodson@bbnc.net