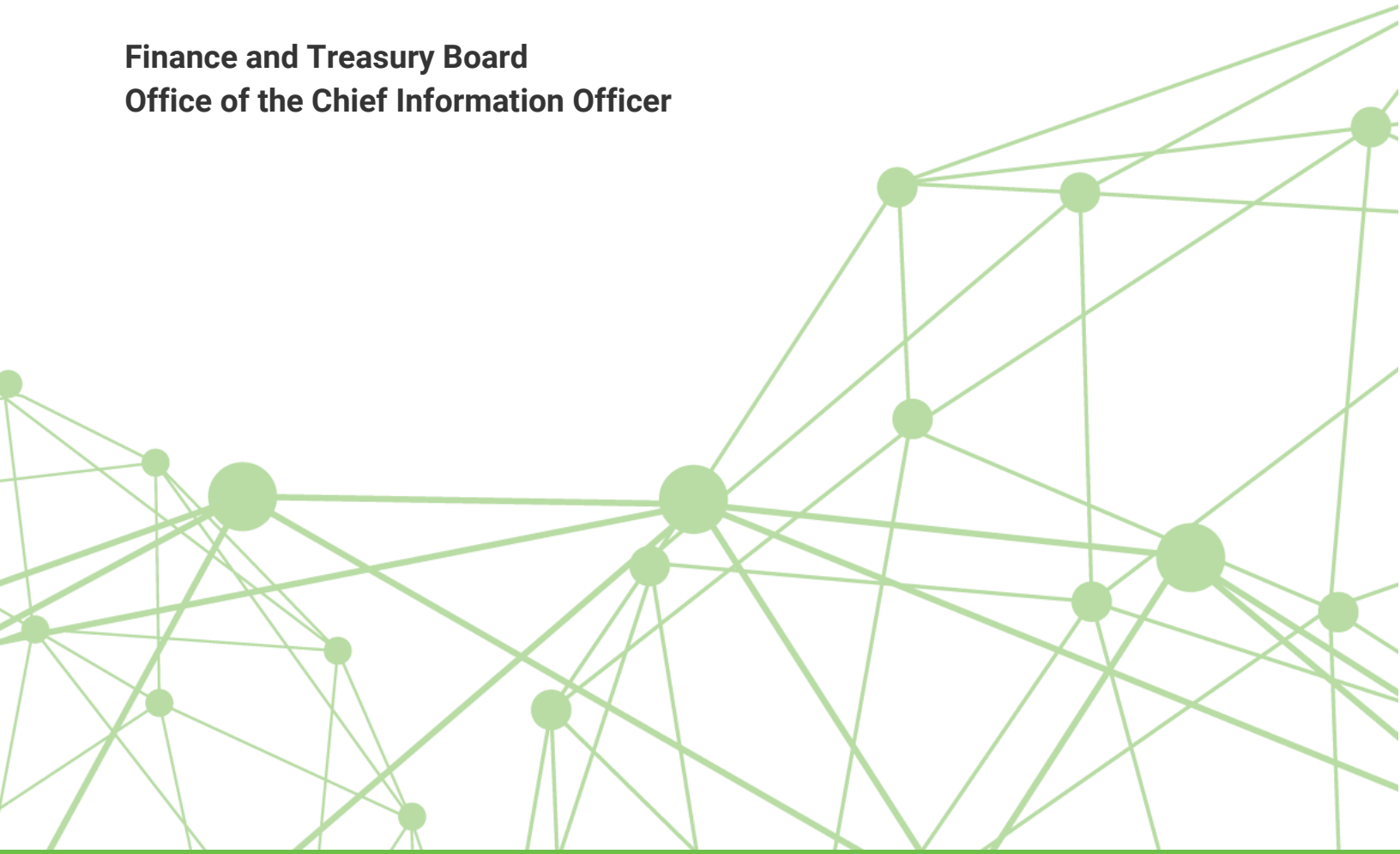
digital NEW BRUNSWICK

Enabling Our Digital Future Securely

Finance and Treasury Board
Office of the Chief Information Officer



New Nouveau Brunswick

Cyber Security Strategy

Contents

Helping to Build a Digital New Brunswick

Cyber security is a key component in building a Digital New Brunswick. This Cyber Security Strategy provides a framework for ensuring the safety and sustainability of our information and systems for all New Brunswickers, whether at work, at home, or at play.

Our approach is simple: Know well and protect enough. We must know our business well and provide the "right amount" of protection to achieve our goals. Anything less leaves us vulnerable, and anything more is waste.

Where is Cyber Security Today?

Cyber security is "the measures taken to protect information against unauthorized access or attack." Technology is continually changing and affecting how we live. From smart phones to life-saving medical devices, our world is becoming very smart. Criminals are using technology to harm us – like stealing our credit card information or hijacking our data and demanding money to get it back. With new technologies, such as artificial intelligence, hackers are launching more sophisticated attacks that are harder to stop.

Our Cyber Future – Trusted, Agile and Solution Focused

We must have solid cyber security to establish trust in a Digital Society. Cyber security must be simple and built in to all GNB services. We will be agile. We will counter cyber attacks quickly and be highly responsive to changing citizens needs. Above all, our approach will help citizens to access services securely in an easy and user-friendly way.

Our Goals for a Cyber-Safe New Brunswick

1. **Protect New Brunswick's information and systems**
   - Information is confidential, trusted and available to citizens when needed
   - Cyber security is delivered effectively and consistently to all of government
2. **Balance cyber risk with benefits**
   - A culture of cyber-safety is in place province-wide
   - Cyber security decisions are based on reliable information
3. **Protect better, smarter, faster**
   - Cyber security solutions are increasingly automated and integrated
   - GNB cyber security solutions adapt quickly to changing threats and needs
4. **Build cyber trust**
   - Citizens trust GNB to deliver digital services safely and securely
5. **Train, gain, retain**
   - All employees are trained on cyber security practices
   - Employees have the skills to keep government information secure
   - GNB has a workplace that attracts and retains skilled cyber security professionals.

Where is New Brunswick Headed?

The 21st century is the digital age. There has been a revolution in how we communicate, how we get to information, and how we do business. From shopping and booking travel, to banking and paying bills, we now expect instant access. We want up-to-the minute information and ease of use. Digital is already playing a central role in our lives and in New Brunswick's economy. That role will only increase. This is an opportunity.

In the digital age, New Brunswickers want to be able to use their smartphone to renew driver licenses or check the results of medical tests. They want to do this anytime, anywhere and on any device. To meet these needs, we are modernizing how we deliver services to the public through a strategy called Digital New Brunswick.

Allowing New Brunswickers to access their personal information online must be done safely and securely. It is vital that government and citizen's personal information be protected so that nobody can access it without their permission. It is also very important that government and citizen's information be accurate and available when needed.

Cyber-Safe is one of the seven core areas of the GNB Digital Strategy and describes how cyber security helps New Brunswick become a digital society in a safe and secure way.

Why Do We Need a Cyber Security Strategy?

The Internet and social media have given criminals powerful tools to attack us. From hacked credit cards to computers infected with viruses, criminals can harm us in many ways. Hackers have access to the latest technologies and their methods are constantly changing.

Cyber security incidents – successful attempts to gain unauthorized access to a computer or computer systems – occur every day (see Figure 1) in governments and businesses. If we are not properly prepared, it can take considerable time to even notice we are hacked.

The message is clear. Cyber criminals are constantly adapting to new technology. Governments and businesses must be equally smart and adaptable to find new ways to meet this threat and to protect our information.

What is Our Vision for Cyber Security?

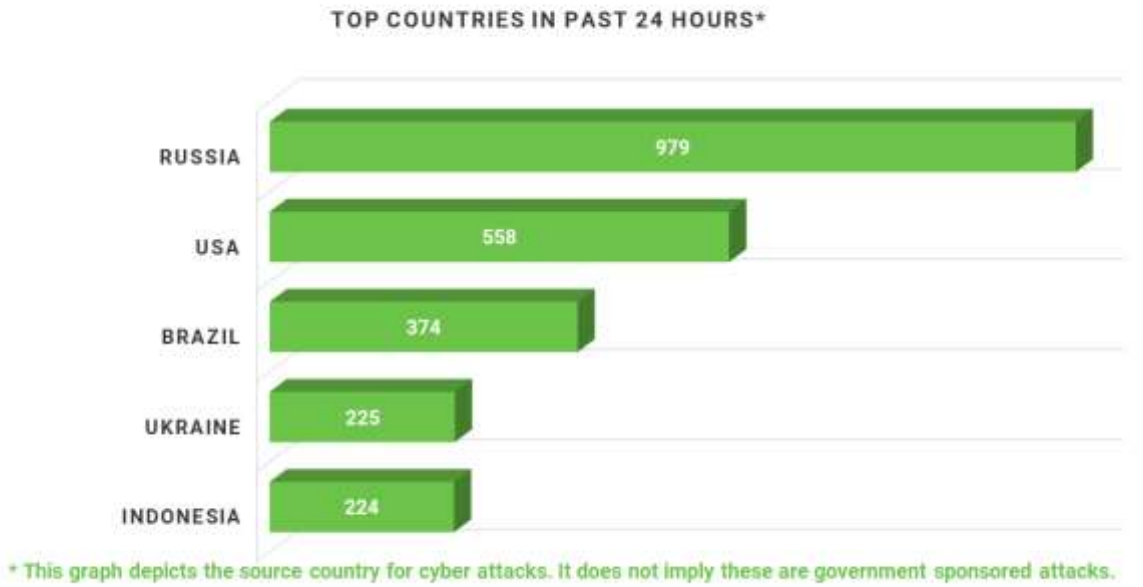
The Cyber Security Strategy will support a Digital New Brunswick. The vision is to provide a safe and trusted environment for New Brunswickers to thrive as a Digital Society.

Digital New Brunswick has five principles. The Cyber Strategy follows all of them:

- We place citizens and businesses at the centre of what we are doing.
- We use accurate and reliable information to make decisions based on evidence.
- We adapt to change rapidly and improve iteratively.
- We work in trusted partnerships.
- We look at the big picture.

In short, NB cyber security will be trusted, agile and solution focused.

Figure 1 – Real time cyber attacks GNB (January 23, 2019 at 8:30 AM AST)



Trusted

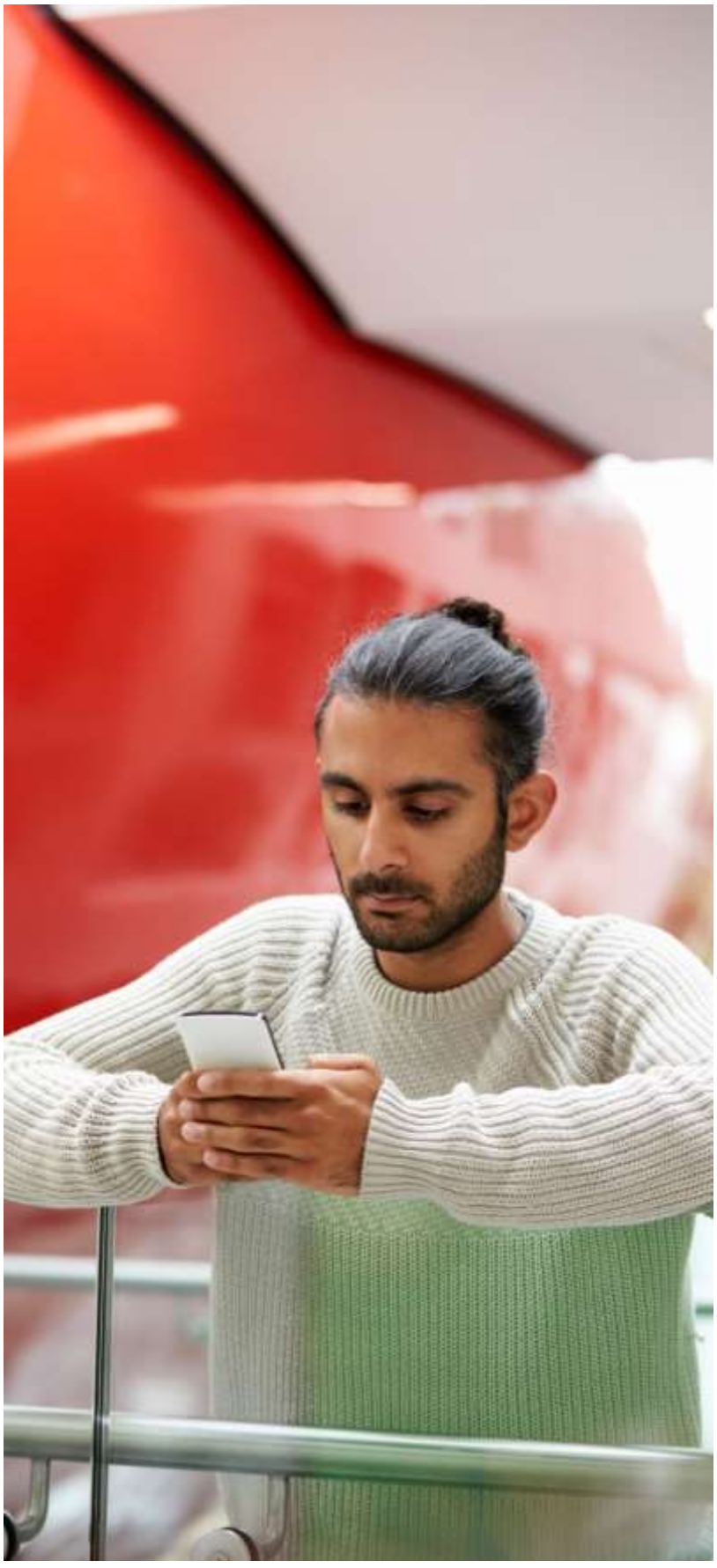
The purpose of this strategy is to provide cyber security that helps citizens and businesses thrive in a digital world. This requires trust. This starts at the top with **strong leadership and direction**. To achieve this, leaders must promote cooperation and communication across all departments at all levels. Having a consistent approach to cyber security across government will require strong teamwork. This will help build trust with all our stakeholders.

Agile

Technology is changing rapidly and cyber criminals are keeping pace. We will address cyber security challenges rapidly and iteratively, improving as we go. We need to work toward smart solutions that use new technology, like artificial intelligence, to automate how we handle cyber-attacks. Our response must swift and effective as our environment continually changes, whether it is a new computer virus or new laws around privacy.

Solution-Focused

In developing cyber security solutions, our goal is to focus on what people need and not just technology concerns. We must strike a balance and address new risks with solutions that meet the cyber security needs of citizens and businesses.



How Was the Cyber Security Strategy Created?

The most important part of developing our Cyber Security Strategy was to focus on our customers. This was done through workshops and meetings held over several months. This allowed us to understand where we are today with cyber security, where we want to be in the future, and realistic goals about how to get there.

Who Are the Key Players?

Everyone has a role to play in cyber safety. By each doing our bit, we collectively reduce risks and increase benefits.

Government of New Brunswick (GNB)

The Government of New Brunswick is responsible for protecting New Brunswickers' data in its care. Some GNB departments and agencies have specific responsibilities.

Finance and Treasury Board (FTB)

Finance and Treasury Board is responsible for providing strategy, policy, monitoring, and reporting services to all other GNB departments and agencies.

Service New Brunswick

Service New Brunswick provides operational support for protecting GNB assets by acting on Finance and Treasury Board strategy, policy and advice.

Department of Public Safety (DPS)

Department of Public Safety handles national and general security related to public safety, emergency management, law enforcement, and critical infrastructure.

Department of Transportation and Infrastructure (DTI)

Department of Transportation and Infrastructure is responsible for the security of government buildings.

CyberNB

CyberNB (an initiative of Opportunities NB) helps build cyber security capabilities in New Brunswick through collaborative innovation between government, the private sector, academia and other jurisdictions.

Post Secondary Education Training and Labour (PETL), Education and Early Childhood Development (EECD)

PETL and EECD are educating New Brunswickers on cyber security and digital literacy.

GNB Employees

GNB Employees are responsible for following cyber security policies and standards which will help them stay secure and deliver secure services to citizens.

Business Community

Businesses are responsible for protecting their devices and information, and supporting critical infrastructure such as telecom, power, transportation, and water and food.

Citizens

We are all responsible for protecting ourselves online, at home and at work. We must keep our devices up to date and only share personal information with those we trust.

What Is the Impact for New Brunswickers?

The GNB digital strategy is designed for all New Brunswickers. Whether they are online or off, citizens will see improvements in their everyday lives.

Cyber security will keep others from seeing or changing our information without our consent, while making it available to us when we need it.

What Are Our Goals?

The following are our strategic goals and expected outcomes for the Cyber Security Strategy.

1. Protect Government of New Brunswick Information and Systems

Outcomes and Key Performance Indicators (KPIs)

- Cyber security is delivered effectively and consistently to all of government
  KPI – % of annual health checks performed on time

- Policies support accountability and transparency of cyber security efforts
- KPI - % of annual policy/directive reviews completed on time

- A robust cyber security program provides guidance to all GNB
  KPI - % of scheduled cyber security assessments completed on time

Actions

- Conduct maturity and vulnerability assessments to continuously improve our GNB cyber security program.
- Publish strategies for Internet of Things (IoT), mobile, cloud and emerging technologies
- Adopt standard cyber security tools across GNB
- Develop a cyber security balanced scorecard
- Develop a cyber-safety model and policy similar to health and safety

2. Balance Cyber Risk With Benefits

Outcomes and Key Performance Indicators (KPIs)

- Cyber security risk is included in the decision-making process.
  KPI – % of scheduled risk reviews completed on time

- Managers are trained on how to manage cyber risk.
  KPI - % of managers trained on cyber risk management

- Senior managers are updated on cyber risks through timely reporting.
  KPI - % of scheduled cyber security reports delivered on time.

Actions

- Create a cyber risk register to manage cyber risk
- Identify practical risk management practices
- Perform an enterprise risk assessment on GNB smart devices (IoT)
- Perform an enterprise risk assessment on mobile technology

3. Protect Better, Smarter, Faster

Outcomes and Key Performance Indicators (KPIs)

- Cyber security solutions are integrated and address enterprise wide cyber security incidents
  KPI - % of incidents handled entirely by the SOC

- Cyberattacks are detected immediately and response is increasingly automated.
  KPI – % of cyber security incidents resolved on time

- GNB has a continuously updated cyber disaster recovery plan

KPI - % of scheduled disaster recovery plans reviewed on time

Actions

- Continuously refresh the GNB Security Operations Centre (SOC) strategy and roadmap
- Expand the SOC to cover all four parts of government and provide actionable threat intelligence.
- Continuously update the GNB disaster recovery strategy and roadmap
- Improve the enterprise cyber security incident management process
- Develop a cyber-crisis management strategy to address novel cyber attacks

4. Build Cyber Trust

Outcomes and Key Performance Indicators (KPIs)

- GNB cooperates with business and academia through CyberNB and others
  KPI – Number of successful partnerships with academic institutions and businesses

- GNB seamlessly cooperates with jurisdictions across Canada and beyond
  KPI – Successful inter-provincial/Federal partnerships

Actions

- Strengthen our ties with stakeholders to improve our cyber security capabilities and better protect our network
- Cooperate with the Canadian Institute of Cyber Security and the Canadian Centre for Cyber Security
- Explore opportunities with Cyber NB around training, information sharing, establishing best practices

5. Train, Gain, Retain

Outcomes and Key Performance Indicators (KPIs)

- All employees are trained often on good cyber security practices.
  KPI - % of GNB employees trained on cyber security.

- Cyber security talent is part of a strategic talent management plan.
  KPI – % of cyber security employee career planning reviews completed on time

Actions

- Implement a Network of Excellence (NOE) for GNB cyber security professionals
- Develop and implement a cyber security training program for all GNB
- Implement performance based cyber training

What Are the Challenges and Opportunities?

Many challenges face us as we look to build trust and protect citizens' information. Every one of those challenges is also an opportunity to serve citizens better.

Challenge: Lack of Cyber Security Awareness

A successful cyber security programme hinges on communicating effective cyber security practices through the organization.

Opportunities: Cyber Security Strategy implementation will include awareness and education, metrics, appropriate responsibilities.

Challenge: Funding

Adequate investment is necessary to achieve the goals in the Cyber Security Strategy.

Opportunities: The Cyber Security strategy identifies key areas where investment is needed to provide the right level of protection for GNB.

Challenge: Lack of Organizational Readiness

GNB must attract and retain top talent to achieve operational targets. We will use technology to address cyber security staffing and skill gaps. GNB will also need foundational elements, including infrastructure and integration, to help implement the Cyber Security Strategy.

Opportunities: Innovative recruitment and training will promote and sustain organizational readiness.

Challenge: Global Cyber Trends/Disruptive Technologies

GNB needs to keep up with changes to global trends and technology.

Opportunities: The Cyber Security Strategy will support faster and better-informed decisions regarding new technologies.

Challenge: Sustainability

Governments and the security environment is continually evolving. We need to continually adapt to sustain our vision.

Opportunities: The Cyber Security Strategy will be revisited on a regular basis to meet the changing needs of government. We will ensure procedures are well documented and employee roles and responsibilities are clearly defined.

How Will We Manage Cyber Risk?

Like any government, GNB manages risks in Health and Safety, Finance, Human Resources, Environment and other areas. We will help GNB business owners identify and manage their own cyber risk.

We will:

- **Guide and monitor GNB to protect information and ensure employees are working safely online**
- **Monitor security trends**
- **Report the status of risks to accountable stakeholders**
- **Use what we learn to refine future cyber strategy and policy**
- **Make it understandable for decision makers**

How Do We Know We Are on Track?

At the heart of our cyber strategy are realistic goals that are within our control and that can be measured. Our approach adopts simple goals that everyone can understand along with simple measures to show our progress.

In Conclusion

The Cyber Security Strategy will help realize a cyber-secure Digital New Brunswick.

It outlines how we will:

- **build trust with our users and stakeholders across GNB and beyond**
- **be agile and adaptive to changing business needs, technologies and threats**
- **be solution focused and help move the business forward**
- **ensure the right measures are in place to provide the right amount of protection**

This strategy will help position New Brunswick to provide best value for cyber security investments.