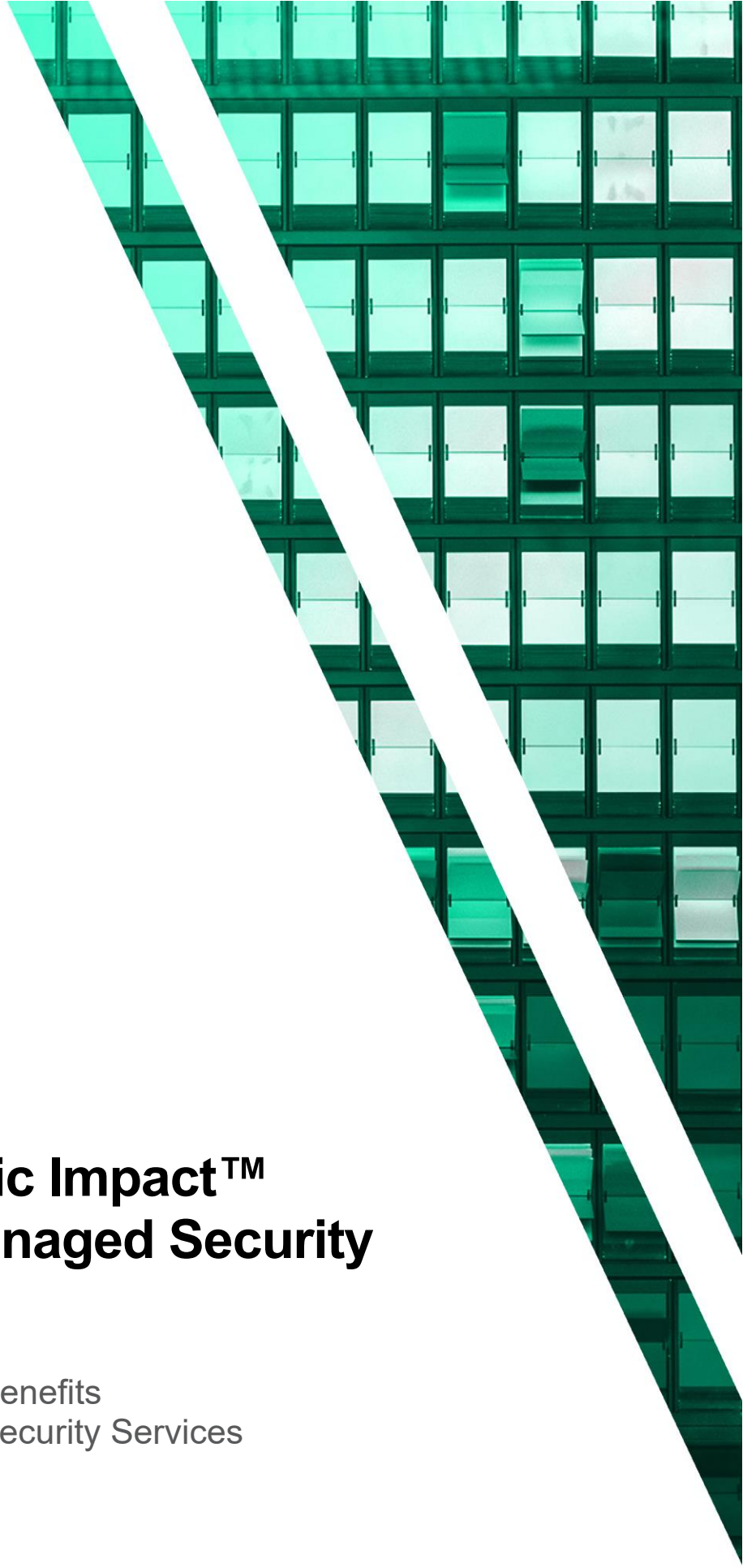
FORRESTER®



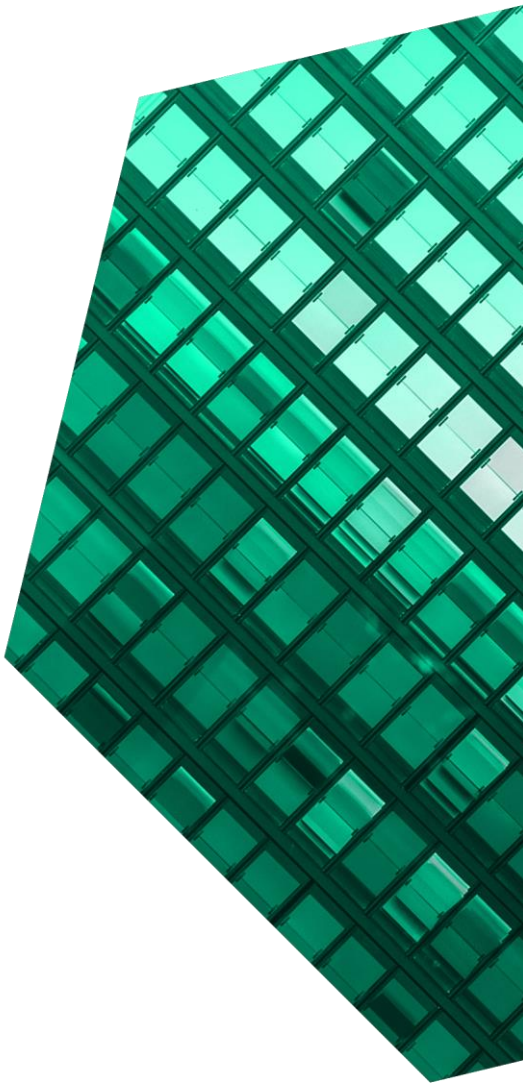
The Total Economic Impact™ Of Bell Canada Managed Security Services

Cost Savings And Business Benefits Enabled By Bell's Managed Security Services

NOVEMBER 2021

Table Of Contents

Consulting Team: Richard Cavallaro
Sam Sexton



ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. For more information, visit forrester.com/consulting.

Executive Summary

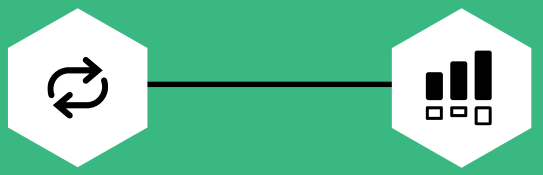
Bell's 24/7 Managed Security Services free organizations from the burden of hiring, training, and retaining scarce security talent, and they decrease the likelihood of a major security breach — all while driving improvements to business continuity, incident response, and total cost of ownership across the security stack.

Forrester research reveals that the average data breach incident costs as much as C$9 million from the response and notification, lost productivity, potential legal actions, regulatory fines, and other potential liabilities. More than three-quarters of businesses have experienced a breach in the last year. With data breaches continuing to increase, data privacy regulations multiplying, and security threats accelerating, managed security services consumer adoption will continue to increase through at least the next two to three years. As the information security threat landscape becomes more advanced and cybersecurity talent becomes scarcer, partnering with a managed security services provider (MSSP) is increasingly attractive for many organizations to provide proactive protection, access to cybersecurity expertise without the need to hire, around-the-clock monitoring, and cost savings on cybersecurity tools.[1]

Bell commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) organizations may realize by deploying their Managed Security Services.[2] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Bell's Managed Security Services on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four customers with Managed Security Services relationships with Bell. For the purposes of this study, Forrester aggregated the experiences of the interviewees and combined the results into a single composite organization.

KEY STATISTICS



Return on investment (ROI)
135%

Net present value (NPV)
C$2.72M

Prior to partnering with Bell for Managed Security Services, the interviewees cited challenges hiring and retaining the security personnel required for an effective cybersecurity function. The security and IT personnel that were available did not have the capacity to provide the constant monitoring and response capabilities required to ensure data security and optimal business continuity. Relationships with several vendors for cybersecurity solutions and capabilities drove a higher-than-desired total cost of ownership (TCO) across the security stack.

After establishing a partnership with Bell Managed Security Services, the interviewed organizations no longer need to source scarce security talent, and they realize improvements to business continuity, better incident response, lower likelihood of a data breach, and reduced TCO across the security stack.

“Whether they come from Bell or the partner vendor who’s providing support, Bell’s experts know their stuff. They’ve been in the industry a long time. They’re very well-seasoned, and they’re all certified. It really goes a long way in building the security trust we need between our two organizations.”

— Director of employee networking services, banking

KEY FINDINGS

Quantified benefits. Risk-adjusted present value (PV) quantified benefits include:

- **Avoided security personnel hires of more than C$2.5 million.** Outsourcing security functionality with Bell Managed Security Services allowed the interviewees’ organizations to avoid cybersecurity staffing increases by leveraging Bell and Bell’s partners’ security and network expertise. Several interviewees reported avoiding more than 200% net additional security hires while alleviating the burden on their HR functions to attract and hire this scarce talent.
- **A 75% reduction in the likelihood of a major security breach.** The interviewees’ organizations reduced the frequency and likelihood of data breaches by greatly improving their cybersecurity capabilities with Bell’s Managed Security Services, decreasing the likelihood of incidents that affect revenue, customer trust, and regulatory compliance. Interviewed decision-makers cited 24/7 monitoring and response as a notable improvement over their prior capabilities.
- **A 70% improvement in business continuity.** With an improvement to security posture, the interviewees’ companies were less likely to experience major or minor security incidents that result in unplanned downtime and business disruption. Improvements to incident response capabilities limit the disruption associated with downtime should it occur.
- **Nearly C$900,000 in total cost of ownership savings across the security stack.** Prior to the Bell Managed Security Services partnership, the interviewees’ organizations relied on a disparate set of security tools and infrastructure from multiple vendors and partners. Consolidating these solutions with Bell allowed these companies to avoid the associated license fees, hardware investments, and personnel time required to manage these solutions and vendor relationships.

Unquantified benefits and flexibility factors. Benefits that are not quantified for this study include:

- **The value of a Bell partnership.** Every interviewed decision-maker cited the partnership with Bell itself as a major benefit. They cited Bell's expertise and market leadership in Canada within networking, its premium partner network, and expert support staff as major boons to working with Bell.
- **Speed of visibility to emerging threats.** Interviewees noted that Bell is very quick to identify new threats, which promotes a sense of confidence within their organization.
- **Protection from future threats.** Interviewees expressed continued confidence in Bell to identify and keep them secure from future threats. This may result in continued business continuity and risk avoidance.

Costs. Risk-adjusted PV costs include:

- **Fees to Bell of less than C$1.9 million over three years.** The interviewees' companies paid annual fees to Bell for their Managed Security Services and the scope of the deployments.
- **Internal personnel requirements of C$157,000 over three years.** Each of the interviewed decision-makers discussed the internal personnel required for interfacing with Bell upon initial deployment and on an ongoing basis

The customer interviews and financial analysis found that a composite organization experiences benefits of C$4.73 million over three years versus costs of C$2.01 million, adding up to a net present value (NPV) of C$2.72 million and an ROI of 135%.

"We've really deepened our relationship with Bell over time. That's what's exciting about the future with Bell. They have so many doors that they can open for us and so many partnership opportunities that align with our security needs."

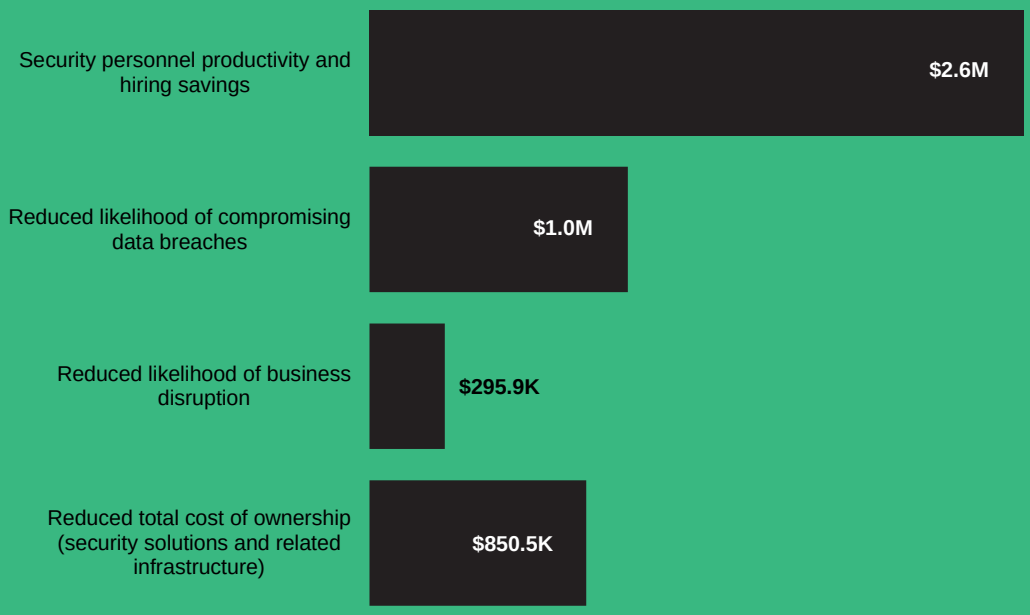
— Chief of staff and senior director, arts and entertainment

ROI
135%

BENEFITS PESENT VALUE (PV)
C$4.73M

NET PRESENT VALUE (NPV)
C$2.72M

Benefits (Three-Year)



TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in Bell's Managed Security Services.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that Bell Managed Security Services can have on an organization.

DUE DILIGENCE

Interviewed Bell stakeholders and Forrester analysts to gather data relative to Bell Managed Security Services.

CUSTOMER INTERVIEWS

Interviewed four decision-makers at organizations using Bell Managed Security Services to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewed organizations.

FINANCIAL MODEL FRAMEWORK

Constructed a financial model representative of the interviews using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewed organizations.

CASE STUDY

Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

The Bell Managed Security Services Customer Journey

Drivers leading to the Managed Security Services investment

Interviewed Decision-Makers

Interviewee	Industry	Region	Revenue
Chief of staff and senior director	Arts and entertainment	Canada	~C$50 million
Director of employee networking services	Banking	Canada	~C$15 billion
Manager, enterprise technology, and CSO	Regional municipality	Canada	~C$1.5 billion
Network operations manager	Software	Canada	<C$5 million

KEY CHALLENGES

The interviewed organizations struggled with common challenges, including:

- **Challenges pertaining to security personnel.** The interviewees related challenges with growing and retaining their security staff amid escalating security risks, requirements, and related management. Some organizations struggled to attract the appropriate volume of security talent to manage these requirements, exposing them to risks from unaddressed needs. Other organizations had difficulty managing their requirements with the limited personnel capacity at their disposal. Furthermore, attrition in the security operations centre (SOC) forced organizations to hire and retrain security employees on their tools and practices, further taxing capacity.
- **A disparate set of tools, services, and infrastructure.** Each interviewee described working with several different vendors across their security stack. This complicated management and interaction between the tools among security staff, while relationships with several vendors fostered inefficiencies from a pricing standpoint.
- **Difficulty maintaining an up-to-date security posture.** Stemming from personnel capacity limitations and a suboptimal set of tools, the interviewees' companies could not always remain up to date on the latest security threats. This exposed these organizations to risks associated with security breaches, including:
  - Unplanned downtime and lost revenue or employee productivity.
  - Brand damage or lost customer trust.
  - Regulatory repercussions.

> **"We are a bank first; we're not a security or IT company. We can't support our own internal 24/7/365 teams like we used to many years ago before we grew."**
>
> *Director of employee networking services, banking*

- **Delayed incident response times.** Several interviewees noted that their organizations simply were not able to reliably provide 24/7/365

coverage in the security operations centre, promoting the risk of a sustained outage or security breach.

INVESTMENT OBJECTIVES

Interviewees searched for a partner that could:

- Bridge the gap between networking and cybersecurity, keeping the organization up to date on the latest security threats or challenges while minimizing disruption across the network.
- Provide 24/7/365 security coverage and immediate response.
- Offer a complete set of cybersecurity solutions and any related infrastructure.

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected. The composite organization is representative of those of the four decision-makers that Forrester interviewed and is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The composite organization is a C$500 million Canadian organization (industry agnostic) that has 20 branch office locations throughout Canada. There are 3,000 employees/endpoints (and growing). The composite organization selects Bell as a managed security provider amid growing cybersecurity requirements and an ever-growing threat landscape given their reach within Canada and full-service set of managed security capabilities.

Deployment characteristics. The composite organization leverages 24/7/365 Bell Managed Security Services across their 20 branch offices and 3,000 users for managed firewall service, managed cloud security gateway, VPN service, distributed denial of service (DDoS) protection, and threat protection and response. Bell also provides (and refreshes) the required infrastructure/equipment for these security solutions as part of the agreement. Prior to selecting Bell as a managed security partner, the organization relied on their very limited security operations personnel, as well as their networking personnel, to manage their growing cybersecurity requirements with extremely limited non-business-hours coverage.

Key assumptions

- **C$500 million annual revenue**
- **3,000 endpoints**
- **Limited security operations personnel**
- **Several vendors for cybersecurity solutions**

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits

Ref.	Benefit	Year 1	Year 2	Year 3	Total	Present Value
Atr	Security personnel productivity and hiring savings	$972,000	$1,036,800	$1,101,600	$3,110,400	$2,568,144
Btr	Reduced likelihood of compromising data breaches	$407,363	$407,363	$407,363	$1,222,088	$1,013,050
Ctr	Reduced likelihood of business disruption	$119,000	$119,000	$119,000	$357,000	$295,935
Dtr	Reduced total cost of ownership (security solutions and related infrastructure)	$342,000	$342,000	$342,000	$1,026,000	$850,503
	Total benefits (risk-adjusted)	$1,840,363	$1,905,163	$1,969,963	$5,715,488	$4,727,632

SECURITY PERSONNEL PRODUCTIVITY AND HIRING SAVINGS

Evidence and data. One of the biggest challenges in IT departments is having the professionals with the right skills and in sufficient numbers to meet business demands. Partnering with an MSSP enables an organization to fill any gaps within their security team or to replace it entirely. An MSSP can also provide access to rare and difficult-to-find specialists when required, such as cloud security specialists, malware analysts, and forensic specialists.[3]

By selecting Bell as a managed security partner, the interviewees' organizations significantly alleviated the burden on their limited security operations resources (or in some cases, networking operations personnel), which avoided the costs associated with hiring, training, and retaining these staff members. Personnel who had previously been managing their respective organizations' cybersecurity solutions and services are able to focus on other business-critical initiatives. Furthermore, working with Bell reduces burden on the organizations' HR functions to source limited cybersecurity talent in the talent market.

- The interviewee at the arts and entertainment organization described an extreme spike in the required security operations and IT personnel capacity once the organization opened its new venue, given a significant increase in external devices on the network on a daily basis. The chief of staff and senior director noted, "We simply wouldn't have been able to manage [it] all internally."
- At the banking organization, the director of employee networking services noted that they would have needed to hire at least 200% more security operations and IT staff to manage their network security before deciding to work with Bell, adding, "If we had to build the capabilities we get with Bell from scratch, we might be looking at upwards of a hundred hires [for our organization]."
- The manager of enterprise technology and CSO at a regional municipality noted that without Bell as a partner, they would need to more than double their current lean security team. "We simply don't need to hire more people to maintain our level of protection. Security people aren't

easy to find. Finding someone who is a good fit is the next challenge."

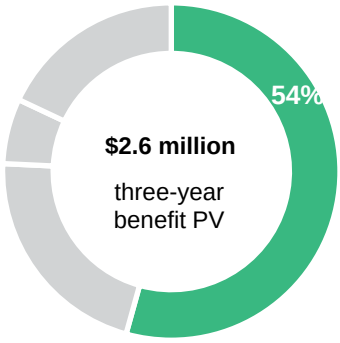
Modeling and assumptions. For the composite organization, Forrester assumes:

- A minimum of 15 security operations/IT FTE resources required if Bell Managed Security Services were not available. This is a conservative estimate for the composite based on interviewee estimates and insight into their before states.
- A 60% decrease in required FTE resources with Bell Managed Security Services.
- An average annual salary of C$120,000 for security personnel.

Risks. This benefit may vary among organizations based on:

- The size and growth of an organization, which affects staffing requirements in IT and cybersecurity.
- An organization's industry as it relates to regulatory requirements or industry-specific personnel demands.
- The skill and capacity of an organization's security and IT resources.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of C$2.6 million.



Security Personnel Productivity And Hiring Savings

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Required security team personnel	Composite	15	16	17
A2	Reduction with Bell Managed Security Services	Interviews	60%	60%	60%
A3	Average annual salary for security personnel	Assumption	$120,000	$120,000	$120,000
At	Security personnel productivity and hiring savings	A1*A2*A3	$1,080,000	$1,152,000	$1,224,000
	Risk adjustment	↓10%			
Atr	Security personnel productivity and hiring savings (risk-adjusted)		$972,000	$1,036,800	$1,101,600
	Three-year total: $3,110,400			**Three-year present value: $2,568,144**	

REDUCED LIKELIHOOD OF COMPROMISING DATA BREACHES

Evidence and data. Limited cybersecurity and IT personnel capacity, disparate sets of security solutions, and a lack of 24/7 monitoring left the interviewees' organizations open to threats, both present and future. Once partnered with Bell, they noted a greatly increased security posture for their organizations. Key reasons cited by the decision-makers include:

- 24/7/365 intrusion and threat monitoring, with near instantaneous response times.
- State-of-the-art security solutions and equipment, such as firewalls, VPN devices, and ISE servers.
- The expertise of Bell's support personnel and Bell's partners.

Interviews with decision-makers revealed the following:

- The director of employee networking services for a bank noted that over the course of their organization's relationship with Bell, there were no significant data breaches or revenue-affecting incidents, which the interviewee attributed to Bell and their partners. They continued: "The collaboration between our staff and Bell is fantastic. A new vulnerability comes out, and we have a notification from them within 24 hours, and a plan shortly thereafter. If it's an immediate threat, we typically have it patched that night."
- The software organization's network operations manager cited improvement of overall threat visibility as a major driver of improved security posture. The organization can also pass this visibility along to its customers, inspiring confidence while promoting a more secure ecosystem.

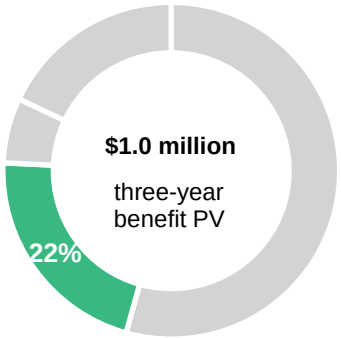
Modeling and assumptions. For the composite organization, Forrester assumes that:

- The average organization based in Canada similar to the composite experiences 1.8 material data breaches per year, based on Forrester Consulting Cost Of A Cybersecurity Breach survey.
- The average loss per breach is C$355,000 based on the size of the composite organization.
- The composite organization reduces its chance of a data breach by 75% once partnered with Bell Managed Security Services. This is a conservative estimate based on the interviews, as several interviewees noted no major incidents at all since securing their networks with Bell.

Risks. This benefit will vary among organizations based on:

- An organization's prior security posture, as it affects the potential improvement to security posture once partnered with Bell.
- An organization's industry and size, as it relates to the likelihood of cyberattack and the potential for losses.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of just over C$1.0 million.



Reduced Likelihood Of Compromising Data Breaches					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Annual number of material breaches (average, Canada)	Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q4 2020	1.8	1.8	1.8
B2	Average cost per breach	Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q4 2020	$355,000	$355,000	$355,000
B3	Reduction in likelihood of data breach	Interviews	75%	75%	75%
Bt	Reduced likelihood of compromising data breaches	B1*B2*B3	$479,250	$479,250	$479,250
	Risk adjustment	↓15%			
Btr	Reduced likelihood of compromising data breaches (risk-adjusted)		$407,363	$407,363	$407,363
	Three-year total: $1,222,088			**Three-year present value: $1,013,050**	

REDUCED LIKELIHOOD OF BUSINESS DISRUPTION

Evidence and data. With improvements to security posture, the interviewed decision-makers expressed confidence in their organizations' ability to avoid unplanned downtime associated with cyberthreats. This allows the organizations to drive higher business continuity, yielding less lost revenue, end-user productivity hours, and customer trust.

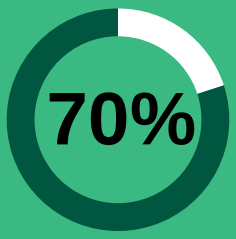
- Several interviewees cited Bell's DDoS protection service as a major driver for their network uptime and business continuity. Furthermore, the manager of enterprise technology and CSO for the regional municipality noted that Bell's DDoS protection allows them to avoid overprovisioning their network (and avoid the associated costs), so they could continue to service their customers and remote VPN employees in the event of a DDoS attack.
- The network operations manager at a software firm estimated an 80% improvement to their historical unplanned downtime resulting from 24/7/365 incident detection and response with Bell.
- The director of employee networking services at the banking organization summarized the importance of their Bell relationship on business continuity: "If one of our branches had to go down because of a security incident on the network, we'd need to take it offline because our business today in each branch is 100% done on the network. Because we have such tight controls, monitoring technologies, and a partnership between our staff and theirs in place with Bell, a rogue device just doesn't happen in our network. If something does get through, we'll know inside 5 seconds. That's how quick they are at alerting us."

Modeling and assumptions. For the composite organization, Forrester makes the following assumptions:

- Losses of C$50,000 per hour, per location. This figure represents lost revenue and lost end-user productivity and has been assumed for the composite based on the interviews and industry-standard metrics.
- Two hours of downtime related to security per year before working with Bell Managed Security Services, which represents just over 99.9% uptime during business hours annually.

- A 70% decrease in this downtime resulting from improvements to intrusion and threat prevention, detection, and response with Bell Managed Security Services.

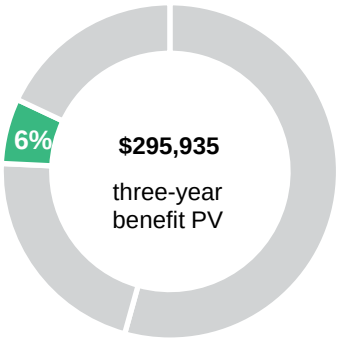
Improvement to incident response times



Risks. This benefit will vary among organizations based on:

- An organization's prior business continuity, as it affects the potential improvement once partnered with Bell.
- An organization's industry and size, as it relates to the likelihood of cyberattack and the potential for security-related downtime.
- An organization's industry and business model, as it relates to the scope of losses during downtime events.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of nearly C$300,000.



Reduced Likelihood Of Business Disruption

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Average hourly cost of unplanned downtime	Composite	$50,000	$50,000	$50,000
C2	Historical average annual hours of disruption-related downtime (rounded, across all locations)	~99.99% uptime on 2,080 business hours annually	4	4	4
C3	Historical annual cost of unplanned downtime	C1*C2	$200,000	$200,000	$200,000
C4	Reduction in security-related unplanned downtime with Bell Managed Security Services	Interviews	70%	70%	70%
Ct	Reduced likelihood of business disruption	C3*C4	$140,000	$140,000	$140,000
	Risk adjustment	↓15%			
Ctr	Reduced likelihood of business disruption (risk-adjusted)		$119,000	$119,000	$119,000
	Three-year total: $357,000			**Three-year present value: $295,935**	

REDUCED TOTAL COST OF OWNERSHIP (SECURITY SOLUTIONS AND RELATED INFRASTRUCTURE)

Evidence and data. The interviewed decision-makers cited cost savings across their entire security stack as a significant benefit of their relationship with Bell as they retire software licenses and security-related infrastructure, as well as avoid personnel hours associated with management of a disparate set

of tools and infrastructure. Common avoided costs included:

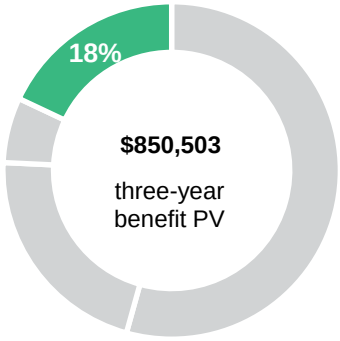
- Infrastructure purchase and refreshes, as Bell provides equipment and refreshes through their partners. The chief of staff and senior director for an arts and entertainment organization estimated a 30% savings from their prior security stack on purchasing efficiencies alone.
- Software licenses for other endpoint detection and response (EDR), security event and information management (SEIM), DDoS protection, and other solutions.
- IT personnel time associated with infrastructure and solution sourcing, refresh, updates, and management of multiple vendors.

Modeling and assumptions. For the composite organization, Forrester makes the following assumptions:

- A yearly infrastructure refresh cost of C$80,000 based on a five-year refresh cycle.
- A cost avoidance of C$150,000 annually on now-redundant security solutions.
- A 75% productivity savings on infrastructure and solution maintenance applied to two IT FTEs at the composite organization.

Risks. This benefit will vary among organizations based on the size and scope of an organization's prior cybersecurity capabilities, as they relate to potentially avoidable costs once partnered with Bell.

Results. To account for these variances, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of C$850,000.



Reduced Total Cost Of Ownership (Security Solutions And Related Infrastructure)					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
D1	Total security-related infrastructure cost	$20,000 per location 20 locations	$400,000	$400,000	$400,000
D2	Annual refresh/maintenance	5-year refresh cycle	20%	20%	20%
D3	Subtotal: total annual infrastructure refresh cost	D1*D2	$80,000	$80,000	$80,000
D4	Subtotal: retired software licenses (AV/EDR/SIEM)	Composite	$150,000	$150,000	$150,000
D5	IT personnel tasked with infrastructure procurement and maintenance	Composite	2	2	2
D6	Reduction with Bell Managed Security Services	Interviews	75%	75%	75%
D7	Annual average salary for IT personnel	Assumption	$100,000	$100,000	$100,000
D8	Subtotal: IT personnel cost reduction with Bell Managed Security Services	D5*D6*D7	$150,000	$150,000	$150,000
Dt	Reduced total cost of ownership (security solutions and related infrastructure)	D3+D4+D8	$380,000	$380,000	$380,000
	Risk adjustment	↓10%			
Dtr	Reduced total cost of ownership (security solutions and related infrastructure) (risk-adjusted)		$342,000	$342,000	$342,000
	Three-year total: $1,026,000		**Three-year present value: $850,503**		

UNQUANTIFIED BENEFITS

Additional benefits that customers experienced but were not able to quantify include:

- **The value of a Bell partnership.** Every interviewed decision-maker cited the partnership with Bell itself as a major benefit. Interviewees cited Bell's expertise and market leadership in Canada within networking, its premium partner network, and expert support staff as major advantages. The director of employee networking services at a banking organization summarized: "With Bell, it's a relationship; it's not a business partnership. We are very close, from all the products and services to the staff. Some days we think of them almost as part of our organization rather than with another company."
- **Speed of visibility to emerging threats.** Interviewees noted that Bell is very quick to

"We're always growing. When we're doing our planning, we need a partner who we know is going to be here in 10 years. There is no other Canadian organization with the depth and breadth of experience that Bell has. Vendors come and go, but Bell will always be a full-service shop. If I could sole source with Bell, I would."

Manager, enterprise technology, and CSO, regional municipality

identify new threats, which promotes a sense of confidence within their organization.

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement Bell's Managed Security Services and later realize additional uses and business opportunities, including:

- **Protection from future threats.** Interviewees expressed continued confidence in Bell to identify and keep them secure from future threats. This may result in continued business continuity and risk avoidance.
- **Flexibility for IT personnel.** Interviewees described several business-critical projects that their IT personnel have been able to undertake since relieved of management of security solutions and infrastructure. Over time, these IT projects may yield additional value to the organization.

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A).

"Our Bell representatives, whether it's our account rep or the technical people, always try to exceed our expectations. They always do what's best for us as the customer. It's a great feeling."

Network operations manager, software

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Etr	Fees paid to Bell Canada	$0	$744,700	$744,700	$744,700	$2,234,100	$1,851,959
Ftr	Internal personnel requirements	$31,500	$50,400	$50,400	$50,400	$182,700	$156,837
	Total costs (risk-adjusted)	$31,500	$795,100	$795,100	$795,100	$2,416,800	$2,008,796

FEES PAID TO BELL CANADA

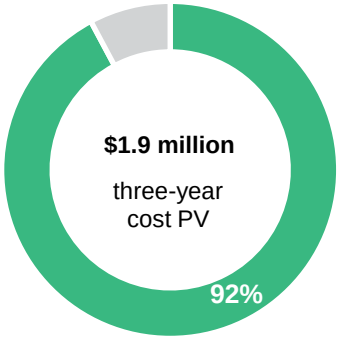
The interviewees' companies paid annual fees to Bell for their Managed Security Services and the scope of the deployments. The below fees have been estimated for the composite organization based on the customer interviews and conversations with Bell. For pricing specific to your organization, please contact Bell.

Modeling and assumptions. For the composite organization, Forrester estimates the following costs:

- Managed firewall and managed cloud security gateway service: C$220,000 annually.
- Managed VPN service: C$132,000 annually.
- DDoS protection service: C$100,000 annually.
- Threat detection and response: C$225,000 annually.

Risks. This cost will vary among organizations based on an organization's size and industry, as it relates to the scope and requirements for deployment of Bell Managed Security Services.

Results. To account for these variances, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of just under C$1.9 million.



Fees Paid To Bell Canada						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Cost for managed firewall service and managed cloud security gateway	Composite		$220,000	$220,000	$220,000
E2	Cost for VPN	Composite		$132,000	$132,000	$132,000
E3	Cost for DDoS protection service	Composite		$100,000	$100,000	$100,000
E4	Cost for threat detection and response	Composite		$225,000	$225,000	$225,000
Et	Fees paid to Bell Canada	E1+E2+E3+E4	$0	$677,000	$677,000	$677,000
	Risk adjustment	↑10%				
Etr	Fees paid to Bell Canada (risk-adjusted)		$0	$744,700	$744,700	$744,700
	Three-year total: $2,234,100			**Three-year present value: $1,851,959**		

INTERNAL PERSONNEL REQUIREMENTS

Each of the interviewed decision-makers discussed the internal personnel required for interfacing with Bell upon initial deployment (as the Managed Security Services partnership began) and on an ongoing basis. Both deployment effort and ongoing effort was characterized as minimal, as Bell and its partners manage most of the initial work and ongoing service.

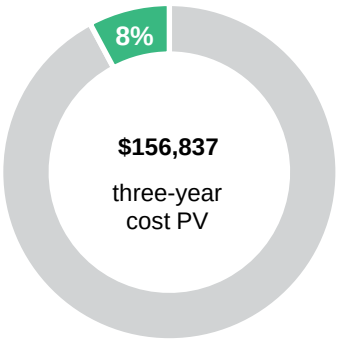
Modeling and assumptions. For the composite organization, Forrester assumes:

- One IT or security resource oversees the initial stages of the security relationship with Bell over the three-month deployment.
- Once the partnership is established, two FTE resources dedicate 20% of their working hours to security-related tasks with Bell.

Risks. This cost will vary among organizations based on:

- The size and industry of an organization as it relates to the personnel requirements for deployment and management of Bell Managed Security Services.
- The skill and capacity of the personnel tasked with implementation and management of the Bell Managed Security Service relationship.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of just over C$150,000.



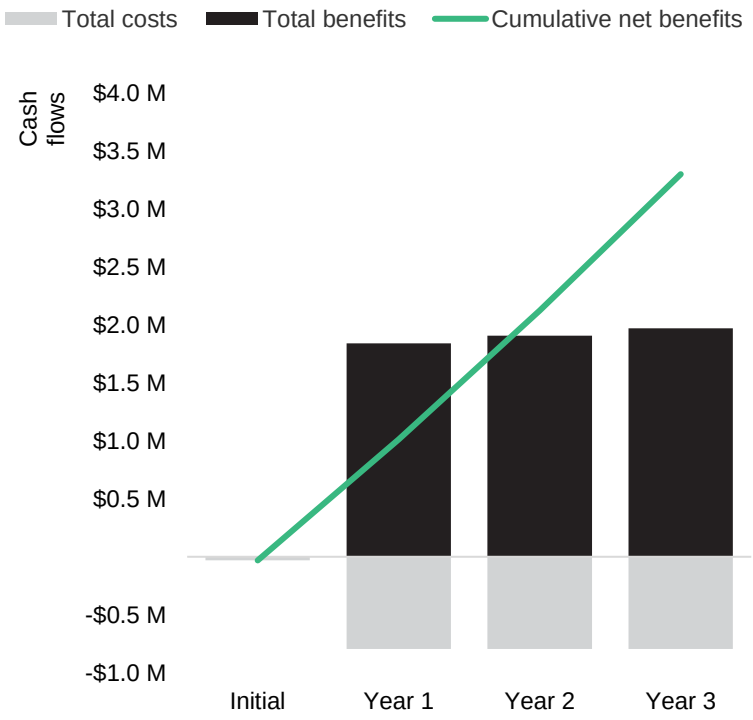
Internal Personnel Requirements

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Personnel required for initial and ongoing security-related tasks with Bell	Initial: 1 FTE for 3 months	0.25	2	2	2
F2	Average annual salary for managing personnel	Assumption	$120,000	$120,000	$120,000	$120,000
F3	Percentage of working hours dedicated to Bell Managed Security Services-related work	Interviews	100%	20%	20%	20%
Ft	Internal personnel requirements	F1*F2*F3	$30,000	$48,000	$48,000	$48,000
	Risk adjustment	↑5%				
Ftr	Internal personnel requirements (risk-adjusted)		$31,500	$50,400	$50,400	$50,400
	Three-year total: $182,700			**Three-year present value: $156,837**		

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI, NPV, and payback period values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Cash Flow Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($31,500)	($795,100)	($795,100)	($795,100)	($2,416,800)	($2,008,796)
Total benefits	$0	$1,840,363	$1,905,163	$1,969,963	$5,715,488	$4,727,632
Net benefits	($31,500)	$1,045,263	$1,110,063	$1,174,863	$3,298,688	$2,718,836
ROI						135%

Appendix A: Total Economic Impact

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

TOTAL ECONOMIC IMPACT APPROACH

Benefits represent the value delivered to the business by the product. The TEI methodology places equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization.

Costs consider all expenses necessary to deliver the proposed value, or benefits, of the product. The cost category within TEI captures incremental costs over the existing environment for ongoing costs associated with the solution.

Flexibility represents the strategic value that can be obtained for some future additional investment building on top of the initial investment already made. Having the ability to capture that benefit has a PV that can be estimated.

Risks measure the uncertainty of benefit and cost estimates given: 1) the likelihood that estimates will meet original projections and 2) the likelihood that estimates will be tracked over time. TEI risk factors are based on "triangular distribution."

The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV Sources are calculated for each total cost and benefit estimate. NPV Sources in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value Sources of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

PRESENT VALUE (PV)

The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total NPV of cash flows.

NET PRESENT VALUE (NPV)

The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made, unless other projects have higher NPVs.

RETURN ON INVESTMENT (ROI)

A project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.

DISCOUNT RATE

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

PAYBACK PERIOD

The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

Appendix B: Supplemental Material

Related Forrester Research

"Recruiting The Right Managed Security Service Providers," Forrester Research, Inc., January 25, 2021.

Appendix C: Endnotes

[1] Source: "Recruiting The Right Managed Security Service Providers," Forrester Research, Inc., January 25, 2021.

[2] Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

[3] Source: "Recruiting The Right Managed Security Service Providers," Forrester Research, Inc., January 25, 2021.


FORRESTER®