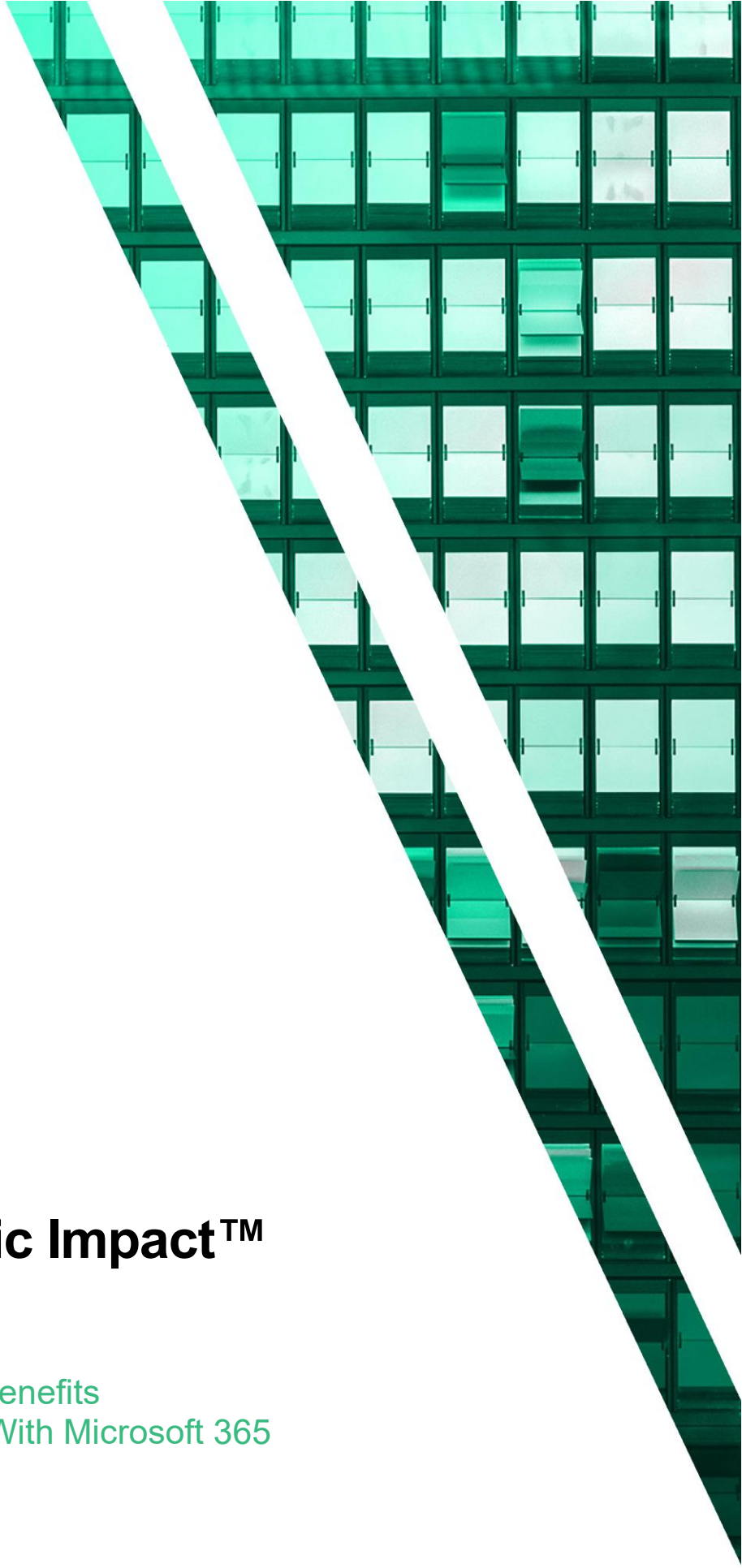
FORRESTER®



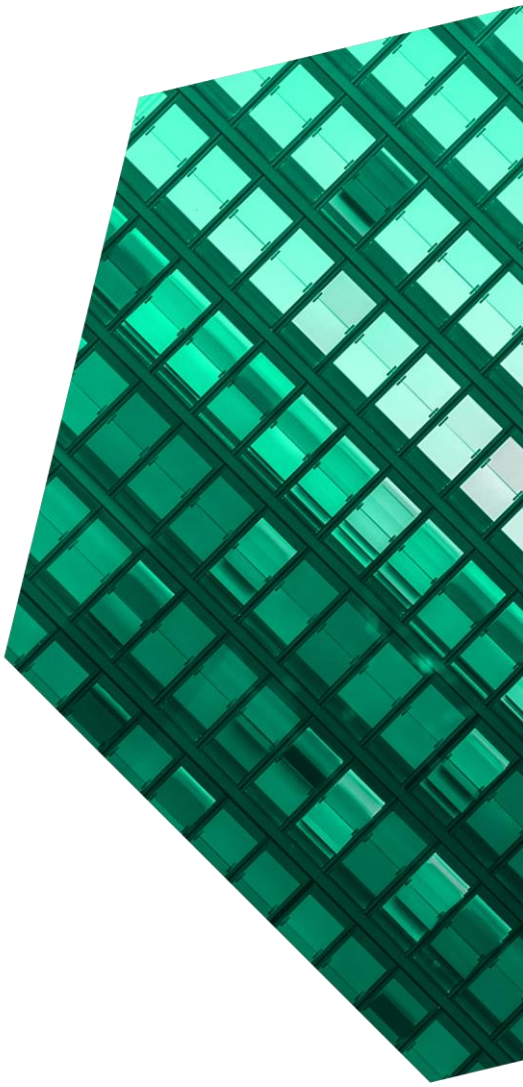
The Total Economic Impact™ Of Mimecast

Cost Savings And Business Benefits Enabled By Using Mimecast With Microsoft 365

JANUARY 2021

Table Of Contents

Consultant: *Kim Finnerty*



Executive Summary

Cybercrime affects every organization no matter the size or type, and it's a threat that is growing and changing constantly. The decision-makers interviewed for this study said their organizations saw clear benefits from the deployment of Mimecast that were over and above the security protections offered by Microsoft 365. This study documents and quantifies how Mimecast protects organizations against threats.

Mimecast commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Mimecast. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Mimecast on their organizations. Mimecast provides cybersecurity and archiving solutions in an integrated, cloud-based platform that protects an organization's people, email and web activity, data, and online brand.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four customers, ranging in size from 6,500 employees to over 65,000, with years of experience using Mimecast in conjunction with their Microsoft 365. For the purposes of this study, Forrester aggregated the experiences of the interviewed customers and combined the results into a single composite organization to model the ROI of the investment.

Prior to using Mimecast, end users at the interviewed organizations experienced spam and other unwanted or malicious email with annoying regularity. They conveyed their frustration through frequent calls to security and email administration teams, and those teams also spent a great deal of time and energy identifying, investigating, and remediating the malicious emails. These activities and incidents led to lost productivity and other costs at all levels of the organizations.

KEY STATISTICS (OVER 3-YEAR PERIOD)

Return on investment (ROI)
225%

Net present value (NPV)
$2.72M

After the investment in Mimecast, customers were able to take full advantage of Microsoft 365 and other productivity and communication systems while also operating more securely. Key results include reduced exposure to internal and external security threats, more effective and cost-competitive archiving capabilities, and improved security behaviors among employees.

KEY FINDINGS

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

- **Prevented losses due to blocked malicious emails saved $1.1 million.** Even after moving to the cloud, the interviewees told Forrester that their organizations continued to experience more spam, phishing, and email-based attacks than decision-makers were comfortable with. Investing in Mimecast to complement the security of their

cloud-based email resulted in a significant reduction in these issues.

- **Streamlined e-discovery efforts returned more than $706,000.** E-discovery can be a time-consuming legal process, and one that could have a critical impact on the outcome of lawsuits in which the interviewees' organizations are involved. The interviewees told Forrester that e-discovery requests previously often took weeks or even months to complete, but Mimecast's tools now handle them in days.
- **Retired on-premises archiving solution saved more than $942,000.** Several interviewees said that after moving their email to Microsoft 365, their organizations opted to initially keep their archives on-premises. The Mimecast platform allowed them to confidently migrate their email archives to the cloud, which let them forego the expense of leasing and maintaining servers.
- **Lowered cost of protecting against fraudulent websites saved $558,000.** Malicious actors are increasingly registering domains and setting up websites to exploit the brand, login, and services of legitimate organizations. Mimecast removed the burden of finding these sites from the security team, and it provided a streamlined, cost-effective takedown service when sites needed to be removed.
- **Reduced email security monitoring time worth more than $613,000.** Prior to deploying Mimecast, the interviewees' organizations employed teams of analysts to identify, investigate, and remediate email-based security threats. With Mimecast in place, the volume of these attacks dropped significantly, and interviewees said they redeployed half or more of these resources to other security initiatives.
- **Decreased costs from employee risky behavior totaled just less than $55,000.** As the last line of defense against social engineering

> **"If a loss could have been prevented, that's on me. We use Mimecast to protect against impersonation, attachments, and a variety of different threats."**
>
> — VP/CISO, healthcare

heavy attacks, an organization's people play an important role in its security. Mimecast's security awareness training program significantly reduced employees' actioning of any malicious emails that made it through the security controls.

Unquantified benefits. Certain benefits delivered real value to the interviewees' organizations, but they could not be quantified for this study.

- **Improved work experience for the security team employees.** Qualified cybersecurity professionals are not easy to find, hire, or retain, and these teams are often under-resourced as a result. By filtering out additional malicious emails before users could act on them or complain about them, Mimecast reduced the workload for team members to a manageable level. This increased their job satisfaction and reduced turnover.
- **Increased end user productivity**. Managing the volume of unwanted emails in employees' inboxes requires daily attention from virtually everyone in the organization. Mimecast allows end users to see and deal with only the emails they decide are relevant, which makes for a smaller, cleaner inbox. End users certainly saved time as a result, but the improved productivity is difficult to quantify.
- **Enhanced confidence in the company's risk profile.** Investing in Mimecast allowed customers to "check the boxes" regarding compliance with national and local regulations. This saves time and increases the chances of success in responding to customer or prospect RFPs, applying for insurance, and streamlining the compliance auditing process.

Costs. Risk-adjusted present-value (PV) costs over the course of the three years include:

- **License fees cost the composite organization $1.15 million.** Mimecast solutions can be purchased on a modular basis to address the threat areas of greatest concern. This allows organizations to build their defenses according to their individual needs and budgets. Fees are primarily determined based on the number of end users an organization needs to protect.
- **Mimecast training and administration for the composite organization total just less than $58,000.** Training for most of the interviewees' organizations focused on security team analysts and involved a few hours of instruction. A part-time system administrator was an ongoing expense for those organizations.

The customer interviews and financial analysis found that the composite organization experiences aggregate benefits of $3.9 million over three years versus costs of $1.2 million, adding up to a net present value (NPV) of $2.7 million and an ROI of 225%.

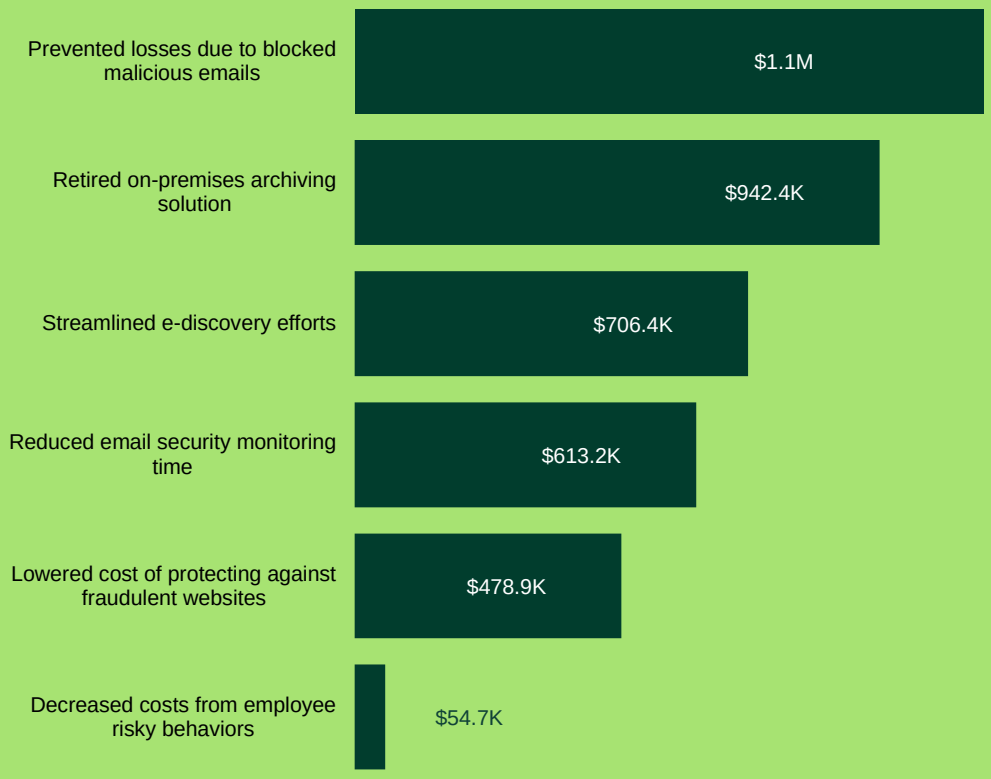
ROI
225%

PRESENT VALUE OF BENEFITS
$3.92M

NET PRESENT VALUE
$2.72M

PAYBACK
<3 months

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 Mimecast.

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 Mimecast can have on an organization.

DUE DILIGENCE

Interviewed Mimecast stakeholders and Forrester analysts to gather data relative to Mimecast and the associated market area.

CUSTOMER INTERVIEWS

Interviewed four decision-makers at organizations using Mimecast 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 Mimecast Customer Journey

Drivers leading to the Mimecast investment

Interviewed Organizations

Industry	Region	Interviewee	Company Size	Email Provider
Financial services	EMEA	Head of security operations	35,000 employees	Microsoft 365
Energy production	APAC	Information security manager	6,500 employees	Microsoft 365
Financial services	USA	CIO	7,000 employees	Microsoft 365
Healthcare	USA	VP/CISO	65,000 employees	Microsoft 365

KEY CHALLENGES

The interviewees' organizations recently moved from on-premises email platforms to Microsoft 365 email. Because email plays such a critical role in malicious actors' attempts to infiltrate IT systems, these customers chose to invest in an additional security layer for their cloud-based email.

The interviewees' organizations struggled with common challenges in this area, including:

- **Finding a balance between security and productivity.** One of the reasons cybercriminals use email so frequently is because it is the communications lifeblood of most organizations. The interviewed security executives are responsible for protecting their organizations from attacks, but they also recognize that attacks could disrupt the flow of business within the organization and with customers and partners.

  This was a difficult balancing act, and one that could result in significant frustration for end users because most people are quite particular about how they manage their mailboxes. Security teams struggled to protect the organizations without disrupting business activity.

> **"Mimecast does a very good job of taking the firehose of junk that gets thrown at companies like ours and getting rid of all the spam, malicious email, and phishing stuff, and giving us a clean feed of email for our users."**
>
> *Information security manager, energy production*

- **Responding to a rapidly increasing volume of e-discovery needs.** The volume and interconnectedness of digital communications across multiple channels can make the process of legal discovery a nightmare for today's legal teams, and some litigants have weaponized it.

  The process can be time-consuming and expensive, involving many hours of research for both security and legal teams. But it must be done properly and thoroughly in order to maximize the organization's chances of success.

- **Protecting the brand in the face of fraudulent email and website activity.** In addition to fraudulent emails, the interviewees said their organizations were increasingly the victims of illegitimate websites meant to defraud customers and business partners by using their organizations' brands. The impact on brand reputation and value — and the associated remediation costs — could be enormous.

  The need to constantly and effectively scan the worldwide web to find fraudulent websites and then build the case to have them taken down placed increasing pressure on already-overworked analysts.

Composite Organization:

- **Business services firm**
- **$5 billion revenue**
- **12,000 Microsoft 365 users**

SOLUTION REQUIREMENTS/INVESTMENT OBJECTIVES

The interviewees' organizations searched for a solution that could:

- Enable them to modernize their office operations with a secure move to the cloud.
- Operate out of the box with a minimum investment in customization, integration, and training.
- Allowed them to complement and build on their investment in Microsoft 365.

Most of the organizations' decision-makers evaluated a number of potential vendors, then chose Mimecast and began deployment — often in phases.

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas of financial impact. The composite organization is representative of the interviewees' companies and is used to present the aggregate financial analysis in the next section.

The composite organization is a multinational provider of business services, including back-office operations such as payroll, benefits, accounting, and legal services. The company has a strong brand, $5 billion in revenue, and 12,000 employees.

Deployment characteristics. The organization operates in multiple countries and uses Microsoft 365 email for its 12,000 employees. The company had initially retained its email archives on-premises after the migration to the cloud, but it now uses Mimecast's archiving solution to move that to the cloud as part of its overall deployment of Mimecast.

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	Prevented losses due to blocked malicious emails	$454,010	$454,010	$454,010	$1,362,029	$1,129,054
Btr	Retired on-premises archiving solution	$378,945	$378,945	$378,945	$1,136,835	$942,380
Ctr	Streamlined e-discovery efforts	$284,050	$284,050	$284,050	$852,150	$706,390
Dtr	Lowered cost of protecting against fraudulent websites	$187,200	$280,800	$280,800	$748,800	$613,217
Etr	Reduced email security monitoring time	$0	$272,079	$338,189	$610,268	$478,945
Ftr	Decreased costs from employee risky behaviors	$22,006	$22,006	$22,006	$66,017	$54,725
	Total benefits (risk-adjusted)	$1,326,210	$1,691,890	$1,758,000	$4,776,099	$3,924,711

PREVENTED LOSSES DUE TO BLOCKED MALICIOUS EMAILS

Evidence and data. Preventing security losses is the primary reason most of the interviewees' organizations invested in Mimecast. The decision-makers are very aware of the increasing frequency and sophistication of email-based cyberattacks, and most of the organizations had experienced more than one successful attack in the recent past.

> **"It wasn't just spam. We had a number of cybersecurity incidents that were related to our email system. More and more of my team's time was being spent on problems relating to email."**
>
> *Information security manager, energy production*

Interviewees told Forrester that, without Mimecast, their organization experienced continuing attacks via emails that contained malicious links and attachments that were sent from imposter addresses, or that employed some new social engineering approach to infiltrate their organization.

- An information security manager with an energy producer said, "Once a week, there's an attack that is good enough to convince someone to cause a loss in the tens of thousands of dollars."
- A CIO with a financial services organization said: "We work with a lot of small businesses, and there's a lot of email correspondence going back and forth. They don't have large IT shops, so there are all kinds of things we get from them that we need to protect ourselves from and to protect them from themselves."
- A VP/CISO with a healthcare organization shared: "A local hospital system was recently the victim of a ransomware attack that took down a number of their facilities. It was a Word

attachment, and we had seen it coming a couple weeks before with Mimecast."

Modeling and assumptions. In quantifying the value of this benefit, Forrester assumes:

- The average cost of a security breach is $343,000.[1]
- The average firm experiences 1.7 breaches per year.[2]
- The composite organization suffers losses from successful phishing-based thefts before deploying Mimecast, where the goal is only to steal money, not to infiltrate IT operations.
    - Approximately once per week, an employee actions an email that costs the company an average of $10,000.
    - Approximately every other month, an employee actions an email that costs the company an average of $125,000.
- Mimecast blocks an additional 35% of malicious emails that otherwise would have been delivered., saving the composite organization 35% of the total cost of these occurrences.

Additional malicious emails blocked

35%

Risks. There are a number of factors that may result in an organization benefitting from this dynamic on a different order of magnitude from the composite. These factors include:

- The number and size of attacks directed at the organization (e.g., malicious actors tend to target financial services firms more than some other industries).

> **"Now it's more about disrupting operations to extort ransom. I think that's the biggest risk for us. Disrupting clinical informatics – from admitting to discharging – can really impact patient safety."**
>
> *VP/CISO, healthcare*

- The number and cost of successful breaches the company experiences before deploying Mimecast.
- The effectiveness of the company's email provider or of any security control already in place and, hence, the incrementality of the solution Mimecast provides.

To account for these risks, Forrester adjusted this benefit downward by 30%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1,129,054.

Prevented Losses Due To Blocked Malicious Emails					
Ref.	**Metric**	**Calculation**	**Year 1**	**Year 2**	**Year 3**
A1	Average cost of security breach	Forrester	$343,000	$343,000	$343,000
A2	Average breaches per year		1.7	1.7	1.7
A3	Annual cost of security breaches	A1*A2	$583,100	$583,100	$583,100
A4	Incremental breach emails blocked by Mimecast	Interviews	35%	35%	35%
A5	Avoided data breach costs	A3*A4	$204,085	$204,085	$204,085
A6	Successful small phishing thefts	1 per week	52	52	52
A7	Cost of small phishing theft		$10,000	$10,000	$10,000
A8	Successful large phishing thefts	Bimonthly	6	6	6
A9	Cost of large phishing theft		$125,000	$125,000	$125,000
A10	Incremental theft emails blocked by Mimecast		35%	35%	35%
A11	Avoided theft attacks	((A6*A7)+(A8*A9))* A10	$444,500	$444,500	$444,500
At	Prevented losses due to blocked malicious emails	A5+A11	$648,585	$648,585	$648,585
	Risk adjustment	↓30%			
Atr	Prevented losses due to blocked malicious emails (risk-adjusted)		$454,010	$454,010	$454,010
	Three-year total: $1,362,029			**Three-year present value: $1,129,054**	

RETIRED ON-PREMISES ARCHIVING SOLUTION

Evidence and data. Some of the interviewees said their organization retained an on-premises archiving solution even after moving its email system to the cloud. This involved a significant ongoing expense in terms of both hardware and software licenses.

- The organizations stored their email archives on physical servers that the organizations owned or leased at a cost. This involved the ongoing cost of service and maintenance contracts. The companies also licensed the archiving software used on the servers.
- One of the interviewees in the financial services industry stated: “We went with Mimecast initially as a tool to help us with email archives, not as a security tool. The solution we were using had crazy pricing, and we needed a much more cost-effective solution for archiving.”

Modeling and assumptions. To determine the value of this benefit to the composite organization, Forrester assumes:

- The organization has maintained an on-premises archiving solution after moving email to the cloud.
- That solution involves server leasing and maintenance contract costs of approximately $20 per user per year, assuming it is in the middle of a six-year capital replacement schedule.

- The organization incurs ongoing annual licensing fees for archiving software of $8 per user.
- It employs one full-time system administrator at a fully burdened salary of $85,050.

Risks. Other organizations may experience the value of this benefit on a different scale as a result of:

- Hardware, maintenance, and licensing costs.
- The number and salary of administrators interacting with the solution in place.

Retired on-premises archiving solution

$942,380

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $942,380.

Retired On-Premises Archiving Solution

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
B1	Archiving hardware and maintenance contract	$20/user/year	$240,000	$240,000	$240,000
B2	Fees for previous archiving software	$8/user/year	$96,000	$96,000	$96,000
B3	On-premises archiving administrator	$63,000+35% benefits	$85,050	$85,050	$85,050
Bt	Retired on-premises archiving solution	C1+C2+C3	$421,050	$421,050	$421,050
	Risk adjustment	↓10%			
Btr	Retired on-premises archiving solution (risk-adjusted)		$378,945	$378,945	$378,945
	Three-year total: $1,136,835			**Three-year present value: $942,380**	

STREAMLINED E-DISCOVERY EFFORTS

Evidence and data. One of the fastest growing legal expenses organizations face now is e-discovery. Before the digital age, legal discovery was relatively straightforward. Each side produced a set of paper documents related to the case. In the digital age, however, the relevant material potentially includes emails, chats, files, databases, websites, and even raw data and metadata. It can involve gigabytes of data and hundreds of hours of labor to find and produce the relevant material.

Mimecast allows legal teams and their email and security teammates to do e-discovery in-house in a streamlined and complete manner. According to one interviewee: “The Mimecast solution is really good. It’s quick, it works, and I can pull the results together easily and give them to the legal team. I’ve been very happy with that. It’s a component that has saved me real money. I spent months on a case a couple years ago putting gigabytes of emails on a hard drive and shipping it to external lawyers. Doing the same thing with the Mimecast tools would take us days now.”

Modeling and assumptions. In modeling the value of streamlining e-discovery work, Forrester assumes:

- The composite organization experiences about 65 lawsuits per year requiring e-discovery.

- Each e-discovery effort requires approximately 100 hours of internal security analyst time before Mimecast archiving is deployed.
- Mimecast reduces that burden to 8 hours of security analyst time per inquiry.
- The organization's security analysts receive fully burdened pay of $104,000 per year.

Risks. The impact risks for this benefit include:

- The number and complexity of lawsuits the organization faces each year will impact the analyst time required before Mimecast is in place.
- The pay rate of the security analysts.

To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $706,390.

Streamlined E-Discovery Efforts

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
C1	Average annual e-discovery requests		65	65	65
C2	Average hours of analyst time required per request	1/2 FTE for 5 weeks	100	100	100
C3	Hours of analyst time required per request with Mimecast archiving	1/2 FTE for 2 days	8	8	8
C4	Fully burdened cybersecurity analyst hourly wage	$76,500 + 35% benefits/2,080	$50	$50	$50
Ct	Streamlined e-discovery efforts	C1*(C2-C3)*B4	$299,000	$299,000	$299,000
	Risk adjustment	↓5%			
Ctr	Streamlined e-discovery efforts (risk-adjusted)		$284,050	$284,050	$284,050
	Three-year total: $852,150			**Three-year present value: $706,390**	

REDUCED EMAIL SECURITY MONITORING TIME

Evidence and data. Each of the interviewees said their organization employed someone to monitor its email security system. Some told Forrester that after the deployment of Mimecast, decision-makers were able to reassign people from email monitoring to other security tasks. Other interviewees said their organization tripled or quadrupled in size with no additional email security hires required to handle the increased volume of email and mailboxes.

- An information security manager with an energy production organization said: "It's saved me at least two full-time employees doing email. We hardly get any calls about spam or mail being wrongly blocked. What most of the team is doing now is investigating phishing attempts and higher-level issues that require their expertise."

Modeling and assumptions. With regard to email security monitoring, the composite organization:

- Employs four analysts to handle the monitoring and remediation of issues on its 12,000 users before investing in Mimecast
- Reduces the team to two during the first year, redeploying analysts to other priority projects.

- Settles at one analyst beginning in Year 2 to address email security issues.
- Pays security analysts a fully burdened annual rate of $104,000.

Risks. The likelihood that other organizations will experience a different level of benefit in the area of email security monitoring is related to:

- The number and complexity of email-based attacks the organization experiences before deploying Mimecast.
- The average salary of security analysts.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $613,217.

Reduced Email Security Monitoring Time

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
D1	FTEs required before Mimecast		4	4	4
D2	FTEs required after Mimecast		2.0	1.0	1.0
D3	Average cybersecurity analyst salary (showing rounded value)	$76,500 + 35% benefits	$104,000	$104,000	$104,000
Dt	Reduced email security monitoring time	(D1-D2)*D3	$208,000	$312,000	$312,000
	Risk adjustment	↓10%			
Dtr	Reduced email security monitoring time (risk-adjusted)		$187,200	$280,800	$280,800
	Three-year total: $748,800			**Three-year present value: $613,217**	

LOWERED COST OF PROTECTING AGAINST FRAUDULENT WEBSITES

Evidence and data. Organizations face an additional security threat that does not necessarily come to them via email. Imposter websites have the potential not only to cost a targeted company money, but also to damage its reputation.

- These false sites can be difficult to find. As one interviewee told Forrester, they may be stood up anywhere in the world, there may be dozens of similar domain names that are perfectly legitimate, and the malicious actor may set up scores of websites at once, but they might carry out illegal activity from only one at a time. Several interviewees told Forrester their organization had a team of analysts scanning the web for imposter websites.
- An information security manager in the energy business shared: “We recently had someone stand up an imposter website that was trying to scam people who wanted a job with us. They were telling people they would get them a job in exchange for $10,000.”
- Once the security and legal teams identify an illegitimate site, they can spend weeks or longer gathering proof that the site operates illegally, communicating with authorities, and actually getting the site taken down.
- Multiple interviewees told Forrester that Mimecast’s service took all of this activity off their team’s plate. Mimecast scans for the imposter sites, investigates them, reports likely offenders to the customer, and then gets the site taken down quickly when authorized to act.

"Before Mimecast, we had to use our local lawyers to try to get this kind of site taken down, and it was almost completely ineffective. Now I just call them and Mimecast jumps through all the hoops and takes down the site quickly."

Information security manager, energy production

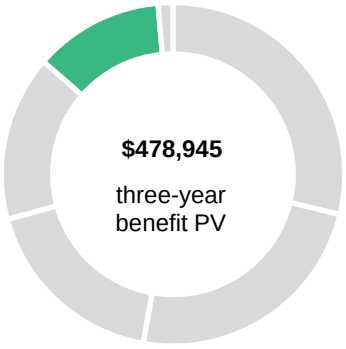
Modeling and assumptions. For this benefit, Forrester assumes the following about the composite organization:

- It requires approximately 3,000 hours of analyst time to monitor the web while searching for and investigating possible imposter domains.
- The organization pays analysts $50 per hour on a fully burdened basis.
- Mimecast's DMARC Analyzer and Brand Protect products reduce that time requirement to 1 hour per month.
- The firm identifies a fast-growing number of malicious imposter websites each year.
- Before investing in Brand Exploit Protect, the firm incurred the following costs for each fraudulent website it detected:
    - 24 hours of legal time at $300 per hour.
    - 150 hours of internal analyst time at $50 per hour (fully burdened) to prove and document the website activity and its damage to the company.
- After deploying Brand Exploit Protect, while malicious sites continue to be stood up, the organization only needs to call Mimecast to authorize action, and Mimecast will remove the imposter site with no further action on the part of the organization.

Risks. The impact risks associated with this benefit include:

- An organization may have more or fewer malicious websites exploiting its brand.
- Rates of pay and seniority level of analysts to monitor and act on imposter domains may vary.
- Firms may or may not engage outside legal expertise in site takedowns.
- Action taken against any given site may involve more or less legal and analyst time.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $478,945.



Lowered cost of protecting against fraudulent websites
12% of total benefits

Lowered Cost Of Protecting Against Fraudulent Websites					
Ref.	**Metric**	**Calculation**	**Year 1**	**Year 2**	**Year 3**
E1	Security team hours to monitor and investigate fraudulent websites	1.5 FTE		3,120	3,120
E2	Security team hours with Mimecast Brand Protect			12	12
E3	Cybersecurity analyst fully burdened hourly salary (showing rounded value)	$76,500 + 35% benefits/2,080		$50	$50
E4	Security team time savings	(E1-E2)*E3		$155,400	$155,400
E5	Number of fraudulent sites taken down per year			10	15
E6	Legal cost to take down fraudulent website before Mimecast	$300/hour * 24 hours		$7,200	$7,200
E7	Security team time to take down fraudulent site before Mimecast	E3 * 150 hours		$7,500	$7,500
E8	Legal and security team time to take down fraudulent site with Mimecast	1 analyst * 10 minutes		$9	$9
E9	Site takedown savings	E5*((E6+E7)-E8)		$146,910	$220,365
Et	Lowered cost of protecting against fraudulent websites	E4+E9		$302,310	$375,765
	Risk adjustment	↓10%			
Etr	Lowered cost of protecting against fraudulent websites (risk-adjusted)			$272,079	$338,189
	Three-year total: $610,268		**Three-year present value: $478,945**		

DECREASED COSTS FROM EMPLOYEE RISKY BEHAVIORS

Evidence and data. The last defense in email security is the recipient and the actions they take. Even if a malicious email makes it through the technical controls, it cannot do any harm unless a recipient acts on it. The interviewees' organizations each engaged in some form of security awareness training to minimize the chance that employees would action a malicious email.

Several interviewed executives said they invested in Mimecast's awareness training, and they reported positive experiences with it. The program consists of a series of animated and humorous short videos that instruct employees how to, for example, recognize suspicious emails and remind them why they shouldn't click the link, open the attachment, or provide their credentials. Because the videos are short and entertaining, interviewees reported that employee engagement was higher than with programs their organizations had used in the past, and they believed their staff was receiving the messaging.

- An information security manager with an energy production organization said: "The awareness training is quite good. The videos are humorous. And we get over a 30% open rate, even with [employees] in the oil field. I've gotten feedback from all over the company from people who tell me they [learned not to] click on some phishing email."

Modeling and assumptions. In modeling the value of this benefit, Forrester made several assumptions about the composite organization's employee

security awareness and employees' willingness to follow guidelines. These assumptions include:

- Before deploying Mimecast and rolling out security awareness training, approximately 15% of employees would have taken an action on a malicious email that would create a security incident, whether large or small.
- After security awareness training and interaction with Mimecast features, that level drops to 2.5%.
- Mimecast and email providers already block 90% of malicious emails, so employees will still be exposed to 10% of the malicious emails directed at the organization.
- This improved security awareness results in a reduction of 1.25% of the organization's total annual risk of email-based losses, as outlined in Benefit A.

"We did phishing simulations and, in the initial ones, 30% of the staff were clicking on the links, and more than half the people who clicked went on to provide their credentials as well."

Head of security operations, financial services

Risks. A given organization may experience the value of this benefit differently as a result of:

- The volume and sophistication of the email attacks directed at recipients.
- The ingoing level of security awareness and judgement among employees.

To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $54,725.

Decreased Costs From Employee Risky Behaviors

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
F1	Average annual cost of email-based attacks	A3 + (A6*A7) + (A8*A9)	$1,853,100	$1,853,100	$1,853,100
F2	Estimated unblocked malicious emails		10%	10%	10%
F3	Percent of malicious emails actioned by employees	30% open; 50% of those action	15.0%	15.0%	15.0%
F4	Percent actioned after Mimecast	10% open; 25% of those action	2.5%	2.5%	2.5%
F5	Reduction in risky behavior	F3-F4	12.5%	12.5%	12.5%
Ft	Decreased costs from employee risky behaviors (showing rounded value)	F1*F2*F5	$23,164	$23,164	$23,164
	Risk adjustment	↓5%			
Ftr	Decreased costs from employee risky behaviors (risk-adjusted)		$22,006	$22,006	$22,006
	Three-year total: $66,017		**Three-year present value: $54,725**		

UNQUANTIFIED BENEFITS

The Mimecast investment yielded several other valuable benefits that the interviewees found difficult to quantify. These benefits include:

- **Improved job satisfaction among a very valuable employee group.** Several of the interviewed executives told Forrester that qualified security analysts are a scarce resource. This is especially true in certain industry sectors and geographic markets. The analysts that do get hired tend to work very long hours, and that leads to declining job satisfaction and turnover. This puts the employer back in the position of having to find a qualified analyst in a tough market.

> **"When the auditors come, email security is one of the major focuses for them. Simply by telling them we have Mimecast we skip a huge part of the process. They don't have to ask about specifics – they know Mimecast does it."**
>
> *CIO, financial services*

- **Enhanced confidence in the company's risk profile.** Virtually every interviewee told Forrester that having Mimecast onboard allows their organization to "check the boxes" regarding compliance with national and local regulations, which can vary considerably by geography and industry. This saves time in responding to RFPs and satisfying insurance requirements. It also increases confidence among clients, auditors, and vendors that data is secure.
- **Improved end user productivity**. Many interviewees related stories about the amount of spam that previously came into mailboxes before implementing Mimecast, and they said it required a small but measurable amount of attention daily from virtually everyone in the organization. Mimecast allows employees quite a bit of flexibility in the way they manage their email. With a little bit of attention early on, employees enjoy a streamlined flow of relevant emails, a cleaner and smaller active mailbox, and the ability to change their email handling or search their personal email archive at any time.
- **More proactive employee attitude toward security**. Interviewees commented that Mimecast's security awareness training provided benefits beyond email security which were beyond the scope of this study. The training touches on topics such as secure handling of badges, laptops, paper copies, and much more.

FLEXIBILITY

The value of flexibility is unique to each customer. There are scenarios in which a customer might implement Mimecast and later realize additional uses and business opportunities. For instance:

- **Increased client retention after employee separation.** While this benefit is more applicable to certain industries than others, it is a significant one. When client-facing people leave an organization, especially when it is by choice, they may take client business with them. Mimecast facilitates proactive steps to minimize damage.

> **"Whenever we have any kind of employee turnover, we go into Mimecast and hand over all their emails to their boss to assess potential damage and work on retaining accounts. Even if somebody deletes all their emails and contacts, it's all still in the archive."**
>
> *CIO, financial services*

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**
Gtr	Subscription fees	$0	$397,635	$500,535	$500,535	$1,398,705	$1,151,211
Htr	Training and administration	$1,680	$22,386	$22,386	$22,386	$68,838	$57,351
	Total costs (risk-adjusted)	$1,680	$420,021	$522,921	$522,921	$1,467,543	$1,208,562

SUBSCRIPTION FEES

Evidence and data. By far, the bulk of the costs the interviewees' organizations experienced were subscription fees paid to Mimecast.

- Fees were based on the number of employees and contractors and the number of services to which the organization subscribed.

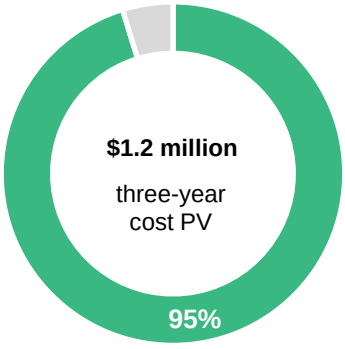
Modeling and assumptions. In modeling the costs for the composite organization's Mimecast subscriptions, Forrester assumes:

- The organization purchases and implements the following Mimecast services in Year 1 for 12,000 employees:
  - Secure Email Gateway with Targeted Threat Protection
  - Internal Email Protect
  - Awareness Training
  - Email Continuity
  - Archive
  - E-Discovery and Early Case Assessment
  - Support: Legendary Customer Support (LCS) Gold
  - Managed Implementation
- In Year 2, the organization adds Brand Exploit Protect and DMARC Analyzer

Risks. The potential risks that could impact these costs include:

- Variability in the number of employees the organization wants to protect.
- Differences in which specific tools the organization decides to purchase and when it deploys them.
- The potential for future price increase.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1,151,211.



Subscription fees
95% of total costs

Subscription Fees						
Ref.	**Metric**	**Calculation**	**Initial**	**Year 1**	**Year 2**	**Year 3**
G1	Initial subscription			$378,700	$378,700	$378,700
G2	Subscription add-ons				$98,000	$98,000
Gt	Subscription fees	G1+G2	$0	$378,700	$476,700	$476,700
	Risk adjustment	↑5%				
Gtr	Subscription fees (risk-adjusted)		$0	$397,635	$500,535	$500,535
	Three-year total: $1,398,705			**Three-year present value: $1,151,211**		

TRAINING AND ADMINISTRATION

Evidence and data. Because the Mimecast solution works primarily by filtering out and blocking malicious emails or by taking down fraudulent websites and domains, it requires very little attention from end users. For the interviewees' organizations, training focused on security analysts who would be interacting with the tool, establishing and tweaking rules, and responding to system alerts. Interviewees told Forrester this was accomplished within half a day.

The organizations also incurred the cost of system administration. Depending on the size of the organization, this may have involved no more than one FTE.

Modeling and assumptions. For this model, Forrester assumes:

- The security team is the only group that requires formal training on how to use Mimecast.
- That training requires about 4 hours of time for each security team member.
- Security analysts are paid a fully burdened salary of $50 per hour.
- A system administrator spends one-quarter of their time focused on Mimecast.
- System administrators are paid a fully burdened hourly salary of $41.

Risks. The costs in this model may vary based on:

- The skill level and pay scale of the security team members and system administrator.
- The ability of individual end users to personalize their mailbox preferences without extensive formal training.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $57,351.

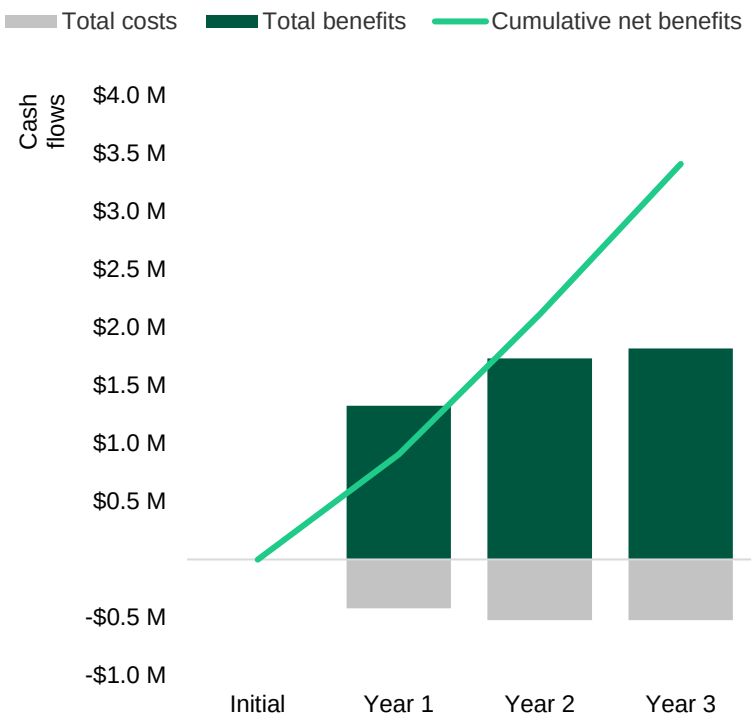
Training And Administration

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
H1	Security team training hours	8 analysts * 4 hours	32			
H2	Security team fully burdened hourly salary (showing rounded value)	$76,500 + 35% benefits/2,080	$50			
H3	Training costs	H1 * H2	$1,600			
H4	System administrator hours	¼ FTE		520	520	520
H5	System administrator hourly pay (showing rounded value)	$63,000 + 35% / 2,080		$41	$41	$41
H6	Administration costs	H4 * H5		$21,320	$21,320	$21,320
Ht	Training and administration	H3 + H6	$1,600	$21,320	$21,320	$21,320
	Risk adjustment	↑5%				
Htr	Training and administration costs (risk-adjusted)		$1,680	$22,386	$22,386	$22,386
	Three-year total: $68,838			**Three-year present value: $57,351**		

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	$1,680	$420,021	$522,921	$522,921	$1,467,543	$1,208,562
Total benefits	$0	$1,326,210	$1,691,890	$1,758,000	$4,776,099	$3,924,711
Net benefits	($1,680)	$906,189	$1,168,968	$1,235,078	$3,308,555	$2,716,149
ROI						225%
Payback period (months)						<3

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."

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

“Prevent Fraud And Phishing Attacks With DMARC,” Forrester Research, Inc., March 31, 2020

Appendix C: Endnotes

[1] Source: “Cost Of A Data Breach,” Internal Forrester Survey Data.
[2] Ibid


FORRESTER®