EMAIL SECURITY IN 2021 - STATE OF THE NATION

A Bytes Market Report
in partnership with Mimecast

BYTES | Smarter together

mimecast

About this Market Report

Email remains the number one vector used by cyber criminals to launch all manner of attacks such as ransomware, impersonation/business email compromise and online brand takeover.

Furthermore, with the level of sophistication of phishing and spear phishing attacks continuing to increase, it is more important than ever that organisations give due and proportionate focus to their email security and email archiving environment.

In the event that systems are compromised via an email-architected attack, personal and customer data, Intellectual Property and brand reputation are the assets deemed most valuable. These are therefore those that criminals target to extract the greatest return from their efforts.

In order to best protect themselves organisations need a triple lock approach:

1. They need to deploy the right technologies and security systems to prevent criminals getting in;
2. They need to train their employees to be extra vigilant and explain the sorts of behaviours and activities to look out for when the criminals come knocking; and
3. They need to invest in backup, disaster recovery and archiving systems to ensure they are able to fully recover from a successful breach.

To understand how organisations are responding to today's email-led threats, Bytes and Mimecast surveyed over 170 UK IT Professionals, in roles ranging from Security Architects and Administators to IT Managers, CISOs and Heads of IT, from a variety of organisations.

This report provides their views and includes further insights and commentary from Matt Compton (Head of Data Management at Bytes), Johan Dreyer (Director of Sales Engineering at Mimecast) and Dr Francis Gaffney (Director of Threat Intelligence at Mimecast).

Report Summary

What is clear from the findings of this report is that organisations recognise the threats they face, but need additional guidance to help them best mitigate against them.

When asked to provide general advice to organisations wanting to improve their security posture, Paul Callaway, SVP of Infrastructure & Security at Cobham, comments, "Use a cloud based email protection service to protect your cloud or on premises mail environment. Implement URL protection, DMARC, AV, attachment protect etc to ensure most threats never reach your mail environment. Implement a security warning banner for all inbound external email alerting users that the email originated outside of your organisation and to be cautious opening attachments or clicking on links".

The survey surfaced some interesting findings:

1. From a business continuity perspective, **Ransomware remains the number one concern.** However, there remains complacency when it comes to protection against general phishing attacks as many organisations consider this threat covered. While this is the case from a technology perspective, all organisations acknowledge that more needs to be done to educate their employees about these threats.
2. **Business email compromise (takeover) is a concern for over 97% of organisations.** These types of attacks aim to: a) fraudulently deceive individuals and organisations into parting with their money and b) steal Intellectual Property and high-value data. They therefore pose a real and present danger that needs sufficient focus to prevent them happening.
3. **Domain/Brand impersonation**, targeting users and staff within organisations using the brand name of their supplier/employer, is deemed less important than other threats, but for some organisations could cause material impact. Organisations that predominately operate in the B2C market are more exposed to these types of attacks than those in the B2B market and therefore need to ensure they are fully aware of the methods used by criminals to exploit their online brand.
4. **Training is the answer, but not the only answer.** Having the right technology in place to reduce the chances of an attack is clearly important, and so too is the need to have the right technology in place to recover from a successful attack. That said, creating a culture of cyber-vigilant employees is essential in the long-term fight against highly sophisticated career criminals. What's surprising therefore is the lack of regular training that's taking place as only 1/3 of respondents state they train their employees at least every 1-3 months.
5. **Configuration, configuration, configuration.** It's widely reported by the likes of Gartner that mis-configuration is the Achilles Heel of most security strategies. Organisations can have all the technology in the world but if it isn't turned on or configured correctly it offers no value. This report highlights key gaps in security provision in this area.
6. **Office 365 is trusted** as a reliable communication and collaboration platform, but Microsoft is less viewed and recognised as a security vendor. Organisations are rightly taking extra measures to ensure their Office 365 environment is properly secured with a multitude of technologies.

From a TECHNOLOGY perspective, how concerned are you about your readiness to face each of the following types of attack?

	Not Concerned	Somewhat Concerned	Quite Concerned	Very Concerned
Phishing/Spear phishing	20.81%	43.35%	24.86%	10.98%
Malware	20.23%	45.66%	25.43%	8.67%
Impersonation, includes business email compromise (BEC) and social engineering	12.14%	43.93%	32.37%	11.56%
Ransomware	8.72%	41.28%	29.07%	20.93%
Denial-of-service	29.65%	41.86%	22.67%	5.81%
Spyware/Credential harvesting/ account take-over	11.56%	45.09%	31.79%	11.56%
Insider Threat	14.62%	54.39%	24.56%	6.43%
Online brand takeover/subversion/spoofing	27.65%	50.00%	20.59%	1.76%

As borne out in our findings, Ransomware is the primary area of concern with half our respondents citing this as a concern. However, as phishing/spear phishing is the primary enabler of Ransomware attacks, these should be considered as much of a concern as the Ransomware itself. The same is true with account takeover. Once again respondents cite this as a primary area of concern (over 2/5 of them rank it highly) however this is also highly linked with phishing.

If organisations have a laser focus on preventing successful phishing and spear phishing attacks, they will significantly reduce their risk profile.

While not reflected in the findings, organisations should be more concerned with the insider threat as this has been the cause of several high level breaches. We would counsel businesses not to forget about data loss, theft and breaches from malicious, negligent or compromised insiders.

It is however encouraging that impersonation is high up the ladder of concern. This is an area that rarely gets much attention and yet presents a material threat to organisations if left unchecked.

The other surprising finding relates to spoofing and subversion as we would expect this to be higher up the concern-ladder, though this may be more to do with the business the respondents are in. Typically those organisations that operate in the B2C market and especially in e-commerce and e-tail have a much greater requirement to protect their online brand and ensure it can't be used against them to exploit their customers.

Our broad spectrum of industry respondents may explain the lack of focus in this group on online brand takeover.

From a PEOPLE perspective, how concerned are you about your readiness to face each of the following types of attack?

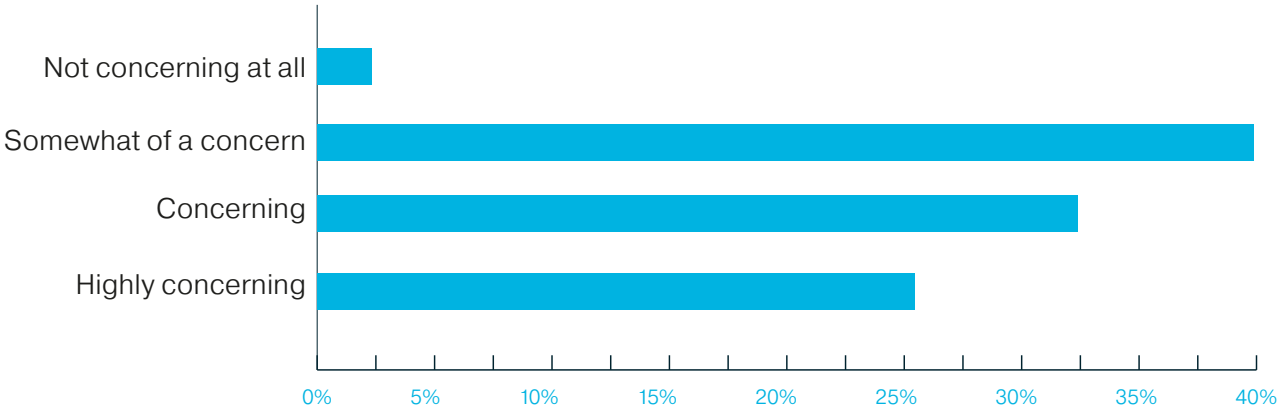
	Not Concerned	Somewhat Concerned	Quite Concerned	Very Concerned
Phishing/Spear phishing	12.21%	37.79%	36.63%	13.37%
Malware	11.70%	44.44%	33.33%	10.53%
Impersonation, includes business email compromise (BEC) and social engineering	8.14%	40.70%	38.37%	12.79%
Ransomware	8.72%	36.63%	37.21%	17.44%
Denial-of-service	38.69%	40.48%	15.48%	5.36%
Spyware/Credential harvesting/ account take-over	9.36%	45.61%	36.26%	8.77%
Insider Threat	20.35%	44.19%	26.16%	9.30%
Online brand takeover/subversion/spoofing	29.82%	46.78%	19.88%	3.51%

When you consider this question in relation to the previous question, these findings paint a false impression and may be leaving organisations avoidably exposed.

Many of the areas of concern, such as ransomware and account take overs, stem from phishing attacks. Whilst technology plays a material part in preventing such attacks, it is inevitable, due to their sophistication, that phishing and spear phishing emails will continue to make it through even the most robust of environments. In these instances employees are the last line of defence, so need to be sufficiently educated to spot and report suspicious emails. It is therefore surprising that only 50% of respondents were either very concerned or quite concerned about phishing in relation to their people. This number should be much greater and will be expanded on further in this report.

Andrew Dodd, Director at Digital Consort comments, “Although the Technical aspect of protection is essential it can only go so far to protect against the human element, it is key that the technical aspect is reinforced with staff training and awareness. Users need to know when to be suspicious of email communication and know the signs / what to look out for to protect an environment. Always, always have a strong backup and recovery policy.”

To what extent do you consider business email compromise as a concern?



The majority of respondents are in one of the two middle categories, so are either somewhat concerned or concerned. This is perhaps not that surprising as this is not a new threat, however, scams in this regard continue to thrive.

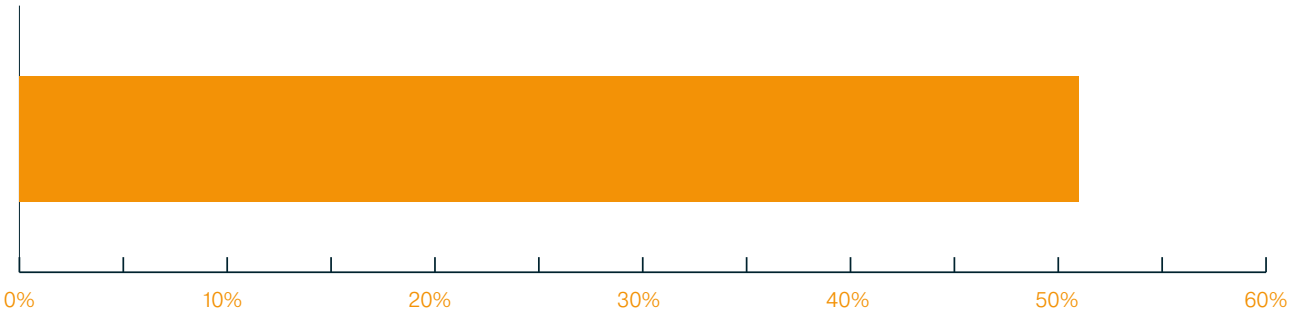
Perhaps one of the most typical is the "Amazon gift card" scam where attackers take over an account (normally of someone senior) and ask a more junior member of the organisation to use the company card to order a number of Amazon gift vouchers. In many cases the request goes unchallenged.

In these cases it proves the value of security training for end users to create a culture where such requests would be checked as standard, as well as the necessary technology to prevent account hijacking.

In addition to financial theft, criminals are taking over email accounts to steal IP and/or personal/customer information. The impact of this will depend on the nature of the business, but organisations that invest materially into Research & Development are advised to understand the full implications of business email compromise activities.

Ahren Stevens-Taylor, Head of Network and Security at Packt Publishing comments, "Foster a security positive culture; encouraging employees to report and be aware of security threats. By attempting to tackle it solely through technology you are going to be stuck in a cat and mouse game with the threat actors."

How confident are you that your employees could spot a fake internal email just by its subject and reference (where nothing is wrong with the domain)?



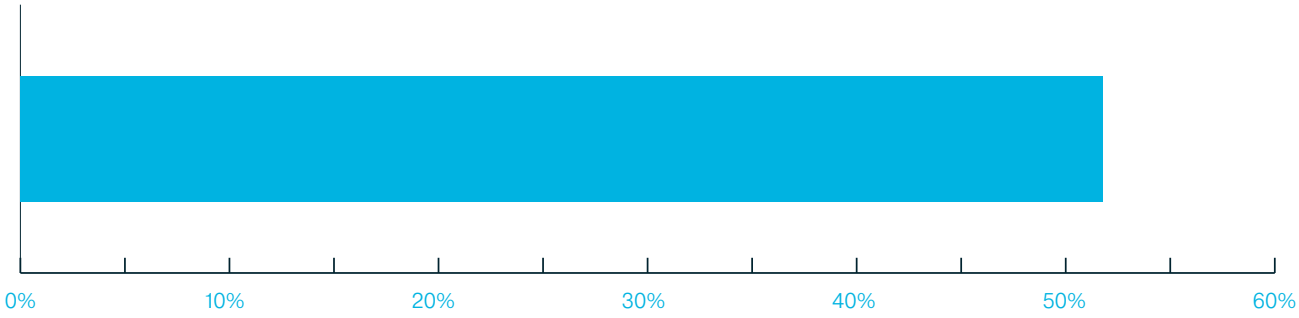
Given the results of the previous question, i.e. that 97% of respondents were either somewhat concerned, quite concerned or very concerned about account takeovers (business email compromise), and also taking into account the findings from the question earlier that asked, "From a people perspective how concerned are you about ... account takeovers) where over 90% of respondents said they were either somewhat concerned, quite concerned or very concerned, the findings of this question should return a confidence score that is significantly lower than 50%.

The challenge however is not just around an employee's ability to spot a fake internal email, but also around ensuring they are sufficiently trained to know what to do if they spot one. Who do they report it to?

The same is true with SMS messages as most people have received scam text messages but most just ignore them rather than report them. If the number is owned and managed by an employer, employees should be more encouraged to report such malicious activity so due warning can be given to other colleagues.

Dimitar Peev, Technical Services and Internal Tools Manager at Genius Sports, comments, "Put people awareness first - training and campaigns. Put tools a close second. No tool will ever protect fully, only employee vigilance can be considered the ultimate protection."

How confident are you that your employees could spot a fake customer email or supply chain attack (i.e. an email where the customer domain has been altered very slightly)?



As per the findings of the previous question, when you consider the complex nature of supply chain emails and exchanges, employees can't be expected to know the domain of every supplier, so a confidence score of 52 is very optimistic.

It is very easy for scammers to buy domains and spin up fake websites that look and respond exactly the same as the ones they are trying to impersonate.

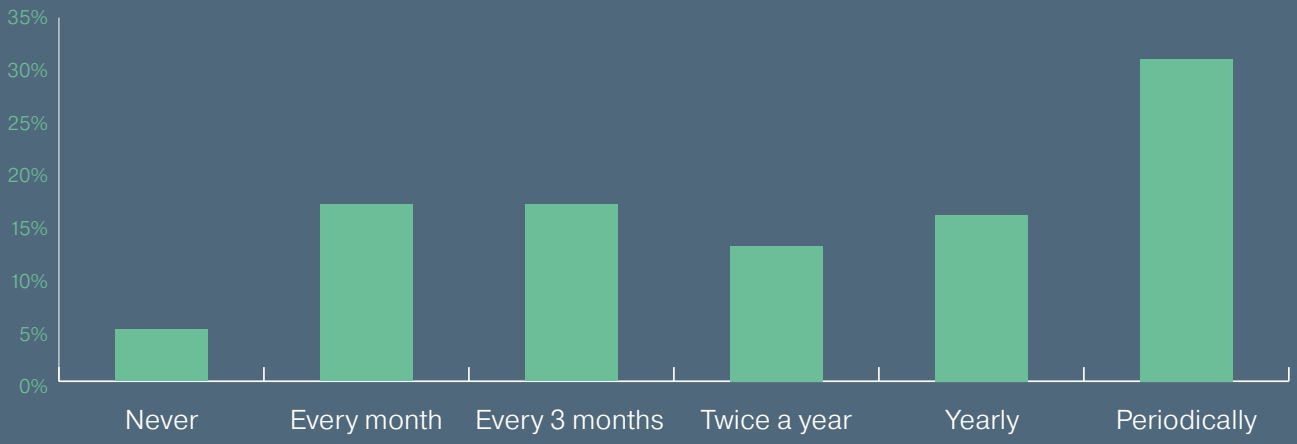
Given the sophistication of these types of crimes, Dr Francis Gaffney says "It's essential that employees receive the most relevant and up to date training to help ensure they are best equipped to spot suspicious emails and keep their general security awareness up to date."

The key focus in preventing such threats is partly technology and partly training so employees are able to be extra vigilant.

Even with this level of optimism, these findings are stark - meaning that IT teams are completely on the fence as to whether their employees would spot email threats, and likely to get it wrong 50% of the time.

So it is clear that advanced technology to block such emails from hitting the inbox in the first place is still very much necessary to help employees.

How often do you train your employees on how to spot the latest cyber threats?



The encouraging finding from this question is that 95% of organisations do train their employees, however only a third train with sufficient frequency - every 1-3 months.

However, as the findings of the previous question show, given the complex nature and sophistication of cyber-attacks, there remains a material shortfall in the amount of necessary training taking place within organisations and the regularity of that training.

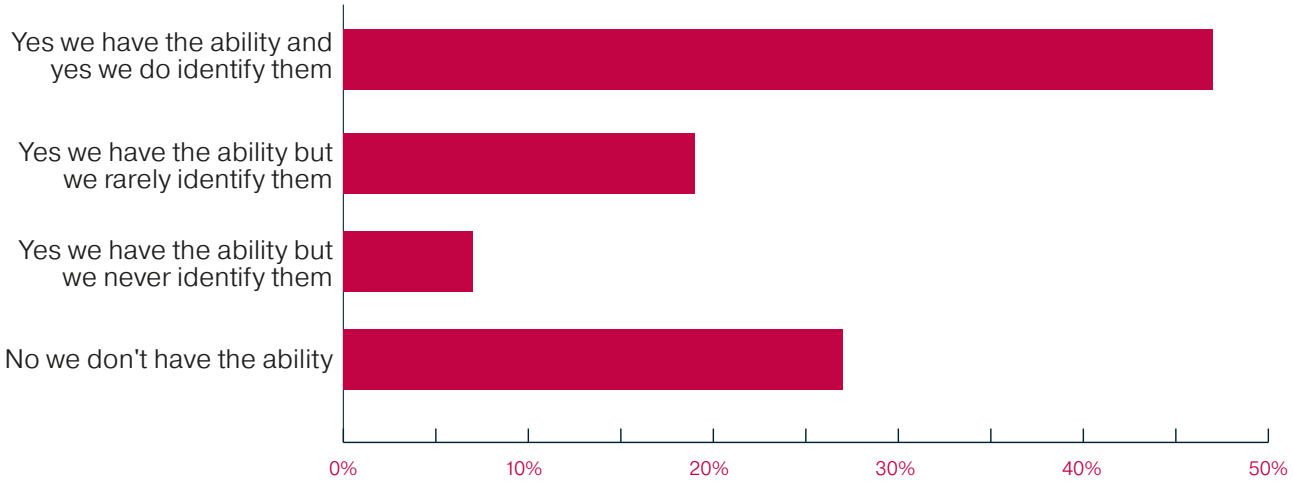
5% of respondents stated they are not doing any training at all. Over 60% are training either twice a year, yearly or periodically, which again is insufficient, particularly given the amount of people now working from home. The detail behind the term "periodically" of course needs to be further understood as if organisations are only training new employees when they join and not after, this is not sufficient to maintain a robust security defence.

Organisations are advised to develop a structured training progamme that delivers little-and-often training to all employees.

To maximise the impact of the training, Johan Dreyer recommends "The training should be varied and tailored so different people who are exposed to different threats, receive training that is relevant and useful to them."

Richard Ward, VP of IT Security at IMI mobile agrees, "Focus on the awareness of the people, they are the last line of defence, a human firewall so to speak. Awareness training is also much cheaper than technology."

Do you have the ability to identify who your riskiest users are, i.e. those most likely to open or click a malicious email/link, and do you identify the users?



52% of respondents either don't have the ability to or choose not to regularly identify their risky users. Given the importance that sensitive data is kept secure and protected, this is a concerning finding as the majority of organisations have no way of being proactive to stop an avoidable breach by honing in on and educating the people most likely to fall victim to an attack.

As organisations are forever being asked to do more with less, it is arguably a much better investment for organisations to use tools to identify and help the most susceptible of employees rather than continue to layer technology on top of technology in the hope it will provide the necessary plaster over the organisation's security environment.

Specialist vendors, such as Mimecast, have the technology to help identify risky profiles and adjust their rights accordingly, thereby helping to limit the chances of a catastrophic attack. If this was an avenue of interest, the first stage would be for Bytes to facilitate a free of charge assessment so all parties can help identify the current threats. Bytes would then be on hand to help define the necessary security processes and policies, then help implement the solution.

Does your email system have the functionality and is configured correctly to prevent:

	Yes we have the functionality and it is configured	Yes we have the functionality but it is not configured	No we don't have the functionality
Malicious URLs	90.06%	8.19%	1.75%
Weaponised attachments	90.59%	7.65%	1.76%
Business email compromise	75.15%	13.02%	11.83%
Unauthorised data transfer	49.71%	30.41%	19.88%
Downtime/Loss of service	68.24%	14.71%	17.06%
Loss of data long term (data retention/regulation)	68.42%	21.05%	10.53%

Unauthorised data transfer presents the greatest risk to organisations as over 50% of respondents either don't have the functionality or haven't configured their systems to prevent it. This could be leaving them wide open to fall foul of their corporate governance, and legislation, such as the GDPR along with revenue loss, brand reputation damage and IP loss.

Given the findings to the earlier question that asked, "From a technology perspective, how concerned are you about phishing / spear phishing", 80% of respondents said they were either "somewhat, quite, or very concerned" and yet over 90% of respondents to this question said they have the functionality to prevent malicious URLs and weaponised attachments. This suggests organisations either don't have the confidence in their email security system or that they don't have confidence in their employee's ability to spot a potential threat. It's most likely the latter.

The other interesting finding from this question is that over 30% of respondents said they either don't have the functionality or haven't configured their systems sufficiently to prevent loss of data long term.

In these instances it's essential those same organisations have a robust email archiving strategy in place to ensure they are able to fully recover their data in an efficient manner.

Bailey Pumfleet, CEO at GriffinCode comments, "Ensure that all available configuration options are locked down to their tightest setting. Don't rely on the defaults being secure."

When it comes to securing your Office 365 environment, how would you rank the following in order of concern?

1=most concerned, 8=least concerned

	1	2	3	4	5	6	7	8
Ransomware	33.12	21.43	12.99	9.09	7.79	5.84	8.44	1.30
Uptime/Availability of service	19.35	10.97	18.06	14.84	8.39	6.45	8.39	13.55
Phishing	15.82	30.38	24.68	9.49	7.59	3.80	5.06	3.16
Employee awareness of threats	13.92	15.82	15.19	14.56	18.35	13.92	5.70	2.53
External brand/ reputation damage	6.45	5.16	8.39	14.19	12.90	16.77	27.74	8.39
Reliability	6.37	11.46	10.83	17.83	18.47	13.38	18.47	3.18
Domain impersonation (DMARC)	3.09	4.32	7.41	14.20	12.96	14.81	12.96	30.25
Archiving	1.25	1.25	2.50	8.75	14.37	24.38	13.13	34.38

What the findings of this question tells us is that people view Office 365 as a reliable collaboration platform but don't have a high degree of confidence in Microsoft as a security vendor, which is why there are concerns over Ransomware and phishing attacks. Two thirds of respondents ranked Ransomware as one of their primary concerns around Office 365 which is the reason Mimecast and Bytes recommend an "onion layered" approach to Office 365 security. The more complementary security layers you can wrap around your 365, the more robust your defence.

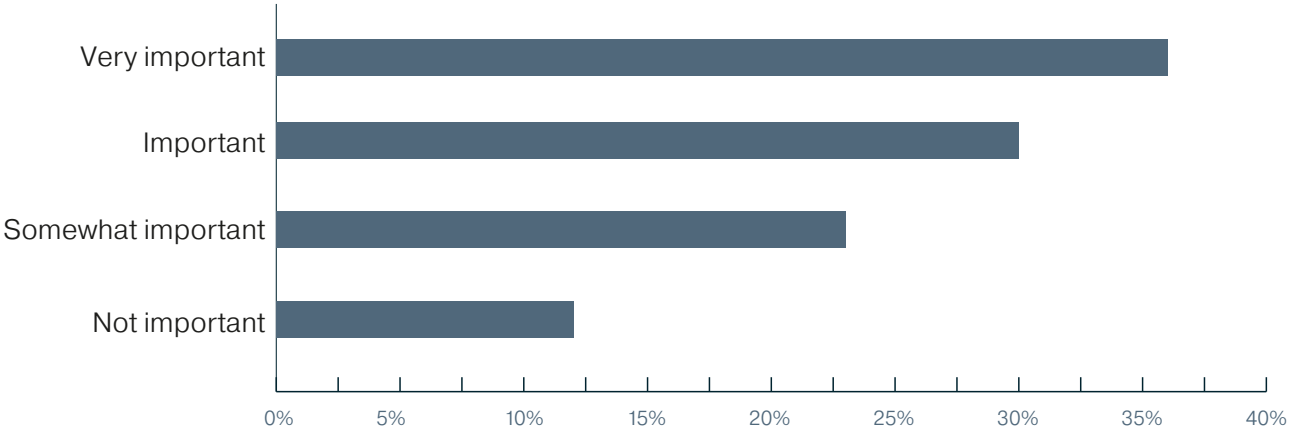
The relatively high concern over uptime/availability of service is often less about the platform itself and more about the influence organisations have over it. On-premises environments are no better or worse when it comes to application availability, but organisations feel more in control over the recovery. In an Office 365 environment however it is not that easy as organisations are reliant on Microsoft to remedy the problem.

Regarding DMARC, Dr Francis Gaffney comments, "While DMARC as a technology has been around for a while, the perception of brand exploitation as a primary concern and therefore adoption of DMARC as a protection method against business email compromise is still quite low. We expect this to change in the near future as businesses need to focus more on preventing the direct impersonation of their digital identity to their business partners & customers in the current environment. With rising e-commerce in 2021 not just in retail but many sectors, we predict this may be an area to watch."

While DMARC is seen as pretty low concern here, it's an area to keep an eye on as it gains traction and those that are getting out ahead of the game are going to be in the best position when it does become mainstream.

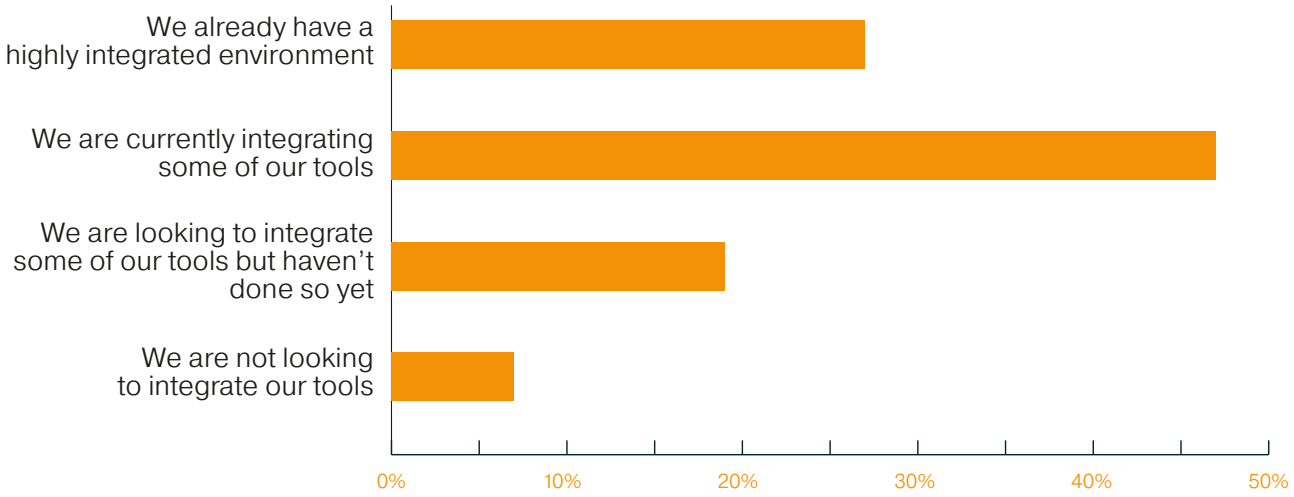
Gus Kilkenny, Infrastructure Manager at J Tomlinson adds, "Implement the protection policies you are given with your Office 365 subscription. Services provided by Mimecast complement Office 365 and add additional features such as Impersonation protect, URL protection & Email Archival."

How important is it that you have a second copy of your Exchange data?



The findings here are self-explanatory, however, it is interesting to note that over a third of respondents state it is either not important or only somewhat important to have a second copy of their Exchange data. From a security and business resilience perspective, this is not necessarily a bad thing, so long as those organisations have made this decision with due care and consideration.

To what extent is your organisation looking to integrate your security tools to help drive efficiencies and better protection?



The findings from this question are encouraging as only by integrating tools can organisations really drive efficiencies and help provide the layered environment they need to protect their business assets.

It is worth noting however, that having a layered approach to security is most effective when the tools are complementary with some, but limited, overlapping functionality. This provides for a robust "multiple locks on a door" approach that helps maximise the effectiveness of the security environment.

Any organisations that need assistance in assessing how their existing security technologies, or indeed new ones, can integrate and combine to create a single threat view where possible, should speak to Bytes. We have extensive experience in mapping and defining the best combination of complementary solutions for partners and assisting in the integration and installation process.

If integration is on the roadmap, it may also be of interest to learn that Mimecast integrates with existing SIEM, SOAR, Endpoint and ITSM applications and other solutions, supporting both pre-configured and custom integrations thereby helping to fast track such plans.

David Price, Head of IT at Curtins, agrees, "Add several layers to your security views. Like a security onion."

Key Takeaways

The findings from this report can be best summarised as follows:

1. **Ransomware is alive and kicking and a growing concern.** No organisation, in any territory of the world, is exempt or immune. If criminals see value in the information an organisation holds, they will stop at nothing until they find it, encrypt it, and hold the organisation to ransom until the ransom is paid. Organisations therefore need to ensure they have a triple lock approach to their data management strategy that includes: 1. Security; 2. Employee vigilance; and 3. Data recovery.
2. **As remote working continues, the attack landscape surface area (and criminal exploitation opportunities) will increase.** Not only are employees more likely to let their guard down while working from home, but criminals will continue to try and exploit less protected networks and mobile endpoints. Education is key to preventing such avoidable breaches, as is having the right technology to provide the necessary layer of protection. The right type of education should be little and often and having a formal, easy to consume security education process in 2021 is a must to protect people properly.
3. **Spear Phishing attacks are becoming ever more sophisticated.** While employees continue to be the last line of defence and the gatekeepers to an organisation's network and assets, criminals will be forever more creative to catch them off guard. Highly refined and complex campaigns are being used to take advantage of COVID-19 and other relevant events in the hope of successfully deceiving an individual and encouraging them to act in a particular way. When successful all manner of criminal attacks will be unleashed, including those involving ransomware and business email compromise - which can lead to financial, I.P, and sensitive data theft. Email systems need to be up to the task to meet these advanced threats, and employees trained to recognise and expect them.

> "Organisations need to ensure they have a triple lock approach to their data management strategy that includes 1. Security, 2. Employee vigilance, and 3. Data recovery." Matt Compton, Head of Data Management, Bytes.

Future Trends

So what can businesses expect to see next as regards their Email Security & protection? What threats and trends are we likely to experience in 2021?

We asked Mimecast's top threat experts to give us their thoughts:

The following Future Trends predictions have been compiled by Dr Francis Gaffney and Johan Dreyer, senior leaders in the world's leading email protection company and Bytes Platinum technology partner, Mimecast, based on their experiences and visibility of global emerging threats and trends.

About Dr Francis Gaffney,
Director of Threat Intelligence at Mimecast

Francis has worked as an analyst in the risk management and international cyber security sectors, for over 20 years with particular interests in strategic policy, geopolitical horizon-scanning, and threat intelligence. His academic background includes a PhD in Defence & Security and four Master's degrees in Information Technology (Management Information Systems), International Law, Terrorism Studies, and an MBA in Strategic Leadership. He has contributed to three books.

At Mimecast, Francis is the Director of Threat Intelligence and is responsible for the generation of policy & doctrine, resource planning, and intelligence output. He leads four separate teams – Threat Intelligence Analysis, Strategic Intelligence & Security Research, Threat Intelligence Risk & Resilience, and Data Science & Overwatch.

Francis is a Chartered Manager and a Fellow of the Chartered Management Institute. He is also a Chartered Chemist, a Chartered Scientist, and Member of the Royal Society of Chemistry.

About Johan Dreyer,
Director of Sales Engineering at Mimecast

Johan is the Director of Sales Engineering at Mimecast where, in addition to heading up Sales Engineering for the UK, he spends most of his time talking to organisations about the challenges and risks that they face. His background is in Information Technology Infrastructure where for more than 20 year's he's been working closely with email and the related services.

His first ever email migration was from Microsoft Mail to Exchange 5.5. Since then he has worked with almost every email platform since as either a consultant, migration specialist or solution architect helping hundreds of businesses design and plan their migration projects.

1. Pattern of Life Analysis

Pattern-of-life analysis includes research of the target to craft specific bespoke lures, such as websites and tailored emails. As part of this analysis, the Cyber Threat Actor (CTA) studies the target's online presence, including their use of social media, to identify social, professional, or family networks, favourite restaurants, hobbies, sporting or musical interests, to better understand how the target can be coerced into leaking data.

An example of how a CTA could exploit online information could be by them reading the organisation's sanctioned biography of the potential victim – this often includes a photograph. Next, the CTA would look for this individual's professional profile on social media (this includes professional bodies, recruitment sites, or for any webinars / conference presentations they may have given). This helps the CTA understand the target's values and interests.

Using online image exploitation tools, the images of the individual can be exploited to see if they appear elsewhere on the Internet. The imagery may also provide valuable metadata, such as the GPS location of where the image was taken (useful for images of the target's home) or what device the image was captured on (useful for identifying the type and model of a smartphone).

Knowing what the target looks like (or where they live) can help confirm the target's other profiles on social media – this could include running/cycling routes, check-ins at local places of interest, or in their network's uploads (whether social, family, or professional images or their activities).

This all assists the CTA in building up insight to the target's activities which will be used to identify vulnerabilities (whether in the technologies they possess, the software those technologies are using, or in the target's personal interests).

Once a vulnerability has been identified that the CTA thinks would be successful if exploited, the method of attack would be crafted to lure the target into compromise. This could be as simple as sending a well-crafted email offering a money off voucher (to one of the target's regular check-ins) as an attachment (with malware embedded in the attachment), to a more sophisticated attack where the target is "canalised" on a pathway (such as open WiFi rather than VPN, or sending data via a non-email method of communication) to their work network avoiding their organisation's cybersecurity measures.

2. Data in Transit

Data in Transit attacks have been a method exploited by CTAs for some time, but such attacks have evolved / been exploited to take advantage of the increased remote working activities due to the COVID-19 global pandemic. Regardless of whether data is communicated via a public or private network, there is a need that this data's confidentiality, integrity and authenticity to be maintained and credible.

If appropriate controls are not in place (and are easily identifiable to a persistent CTA), then this data can be readily accessed / modified by unauthorised CTAs. Such methods include:

- Man-in-the-middle (MITM) attack
- MITM SSL attack
- DNS spoofing attacks
- Baseband attack (for GSM baseband processors)

A MITM attack often intercepts traffic by presenting a spoofed certificate to the target's client to impersonate the server, inducing the target's client to disclose login credentials to the "false" server or even allow the interception

of all communications between the target's client and server. Many users recycle or reuse their passwords and so the CTA can use this information to exploit other accounts the target may have.

An SSL attack on the target's mobile devices is possible when the target's mobile application does not implement SSL (as is often the case). As a result, the application will connect, authenticate, and transmit data in plain text over the network (where a standard MITM attack would be able to recover this data). This attack can also be possible if the mobile application does not properly verify a SSL certificate (where it is implemented).

In DNS spoofing attacks, the target's device is "tricked" into interpreting that a hostname is associated with a specific IP address (when it is not). This would then connect any device responding to the desired hostname leading to the target's login credentials being sent to the "false" host.

A baseland attack focuses on a cellular modem baseband firmware which can allow "privileged" access to the device.

Example

The increased use of cheap, and readily available, "WiFi pineapples" (first released in 2008 but popularised by television programming) allows a CTA to launch potentially easy MITM attacks against home / unprotected WiFi networks. The pineapple allows the CTA to capture unencrypted passwords passed across networks by inserting it between the target's device and a legitimate WiFi access point. In this scenario, the pineapple "pretends" to be a legitimate access point so the target's transmitted data is visible to the CTA.

Need Help to Find and counter the latest Email Threats?

If you think your email system or email domains may be vulnerable to attack, Bytes offers three assessments that can help you size the potential threat and provide a remedial path.

We offer a variety of FREE Assessments

Email Threat Risk Assessment

Bytes **Email Threat Assessment** is a quick, painless way to gain full visibility of how your current email protection solutions are dealing with new and emerging threats, both on premises and in the cloud.

Understand your current attack exposure and receive expert guidance on strengthening your email defences.

Email Compromise Assessment

Email fraud/business email compromise is costing companies billions. Attackers are adept at targeting employees, customers & partners using your brand or domain to exfiltrate money or data. Fight back against the fraudsters.

Bytes **Email Fraud Assessment** will show you exactly how your domain/customers are being exploited right now and the steps you should take now and next to address this.

Phishing Susceptibility Assessment

Phishing attacks have risen 667% since Feb 2020. It has never been more vital to empower people to avoid falling victim.

Target your security awareness efforts in the right places with Bytes **Phishing Susceptibility Assessment**. It pinpoints those most likely to be exploited by phishing & fraud and provides you with concrete advice and tailored tools to best equip those high risk individuals to protect themselves (and your data).

What you can expect

- ✓ **Risk Free – Minimal internal resource required**
- ✓ **Support from expert engineers throughout**
- ✓ **Remediation steps and guidance provided**
- ✓ **Quick and easy set up**
- ✓ **Immediately applicable - Uses real data/known attacks**
- ✓ **Ideal for remote working**
- ✓ **Free of charge and with no obligation**

Need help migrating your email system to the cloud?

Migrating email to the cloud sounds like an obvious move for organisations looking to accelerate their digital transformation. The business case is compelling. However, enterprises are cautious about migrating. So what's holding them back?

We understand the Barriers – and how to Overcome them – Cost Effectively

It's no wonder that organisations look to outside expertise when migrating. But it's essential that help comes at a reasonable price — and IT teams still feel completely in control.

Bytes and Mimecast understand this and provide assistance throughout your whole journey (particularly in those all important early days) to ensure you quickly understand the resource and financial impact of any migration up front. With our proven **5 Step Migration Success Process**, businesses can get the guidance, advice, expertise and execution support they need so their cloud migration succeeds first time.

3-Step migration success process

Step 1 **Discovery Workshop**	Step 2 **Technical Workshop**	Step 3 **Migration Plan**
– Identifying and documenting current & desired states	– Fully scoping technical elements of archive & data migration	– Your personalised transition plan incl. resource planning, timelines & costs

Our support covers every step and milestone of your migration process, both conceptual and practical, from day one right through to project completion. We work hand in hand with you on all of the following critical elements of a smooth migration:

- ✓ Defining what to migrate (PST files, OneDrive, archives)
- ✓ Dependency checking of key applications
- ✓ Opportunities to retire applications
- ✓ Storage consolidation prospects
- ✓ Archive rationalisation
- ✓ Assessing bandwidth availability
- ✓ Selecting the right migration option
- ✓ Active Directory Synching
- ✓ Effective licence assignment
- ✓ Planning for backup and recover

Seeking a total solution for email migration and archiving, so you can get to the cloud far more easily?

With Bytes and Mimecast, it's now possible. We combine market leading technology with a process proven to save money and ease administration burden. You lift a huge burden off your IT team, overcome a host of migration challenges, streamline the process and get a world-class archive solution to boot.

Proven Process which Delivers Quickly

Mimecast Simply Migrate, makes the migration process faster, thanks to its unique architecture, ease of use and integration with the Mimecast Cloud Archive. Plus, eligible organisations can migrate up to 30TB of data free of charge.

Technology with an Attractive TCO

Mimecast Cloud Archive, is the ideal home for corporate email in the cloud. A Gartner 'Leader' for four years' running which delivers a total cost of ownership that's 40-60% less than legacy solutions.

A closer look at the Key Benefits

Simply Migrate takes you to the cloud and delivers:

- **Speed:** Migrate faster due to unique architecture, ease of use and integration with the Mimecast Cloud Archive.
- **Over-the-wire data streaming:** Eliminate time consuming drive shipping, replacing it with same day config and data shipping. Simply extract and process data locally and send the data, encrypted securely, to Mimecast Cloud Archive.
- **Savings:** Flexible cost models reduce your capital expenditure. Avoid paying for the full amount of data extracted from the legacy environment, which might include uncompressed data volumes, duplicative and damaged data sets.
- **Reduced complexity:** connectors to well-known legacy archive vendors.
- **Visibility:** You can monitor the migration process, end to end, with full reporting available.

When you arrive, Mimecast Cloud Archive provides:

- **Financial advantages:** TCO is 40-60% less than legacy solutions. Bottomless archive - no storage fees or overage charges.
- **Versatility:** Support for a wide range of data types, including email, files, instant messaging, and third-party applications.
- **Improved e-discovery:** Industry-leading search capabilities deliver guaranteed results across millions of records in seconds.
- **Self service and control:** Legal, compliance teams and others use intuitive tools and mobile apps to access emails. IT teams are freed up, but stay in control. A single, cloud-based console simplifies oversight and maintenance dramatically.
- **Governance:** Compliance and supervision capabilities dramatically simplify the enforcement of standards by automatically applying company-configured policies.
- **Continuous innovation:** Multi-tenant infrastructure allows for rapid innovation so you keep pace with changing requirements.

About Bytes

Bytes provides leading insights, expertise and practical help to over 3,600 organisations nationwide. We enable effective and cost-efficient technology sourcing, adoption, security and management of software, hardware and cloud services.

Our UK business began in 1982 and has grown profitably each year to reach a turnover in excess of £500m, making us one of the largest software services and solutions businesses in the country.

The most important aspect of our business is our people. We value initiative, teamwork and achievement. Together, we focus on providing the highest levels of service so we can deliver our ultimate goal – customer satisfaction and success.

Our customers include leading brands across retail, media, finance, manufacturing, legal, healthcare and the public sector.

We work closely with the majority of IT vendors and are delighted to regularly receive honours from them in addition to being named a Sunday Times Best Company to Work For 2020.

About Mimecast

Mimecast empowers you with a holistic approach to cybersecurity designed to secure, preserve and continue the flow of information via email. We prepare you for every stage of an attack by: Ensuring the right security services are in place before an attack happens; Providing a durability plan to keep email – and your business operations – running during an attack or failure; and Providing the capability to recover data and other corporate IP after an incident or attack occurs.

Our broad-based, multidimensional cyber resilience strategy covers everything you need to stay ahead of today's evolving threat landscape – all from a single cloud platform.

To understand how Bytes and Mimecast can help you develop and enhance your Email Security Strategy, get in touch and start a conversation today.

BYTES | Smarter together

UK Head Office

Bytes House
Randalls Way
Leatherhead
Surrey
KT22 7TW

T 01372 418 500
E tellmemore@bytes.co.uk
W www.bytes.co.uk