Image credit: matlas jaramillo via Flickr

What will be the single biggest security threat of 2016?

- on December 08 2015

Security is always a huge topic in IT but, with high-profile breach after high-profile breach, it has really hit the headlines this year. So, what do experts think the single biggest security threat of next year will be?
Well, to find out we crowdsourced opinion by asking individuals to sum up their views in one sentence. Of course, it doesn't always work out. Many people exceeded the sentence limit – so we cut their answers back. Whilst as always, others clearly focused on their company's own area, at the expense of the big picture. But what we ended up with was a decent straw poll of industry views.
Finally, it is very hard to catalogue 74 "unstructured" responses into anything clear-cut. So, what we've done is divide comments into nine very loose categories and listed them below.

People – (14 responses) this was the single most popular at 19%
Data – (8 responses)
New-fangled blackmail – (6 responses)
It, the laggard – (6 responses)
Hacktivism and espionage – (6 responses)
The Internet of Things – (6 responses)
Confusion and the wider business – (4 responses)
Specific threats – (6 responses)
Other comments – (18 responses)

Perhaps the most interesting thing that emerges from all this is that many of these comments aren't really anything to do with technology at all. The majority are social and human issues… which is why they're so hard to predict.
We've listed all responses below so you can form your own opinion.

People

Cliff Moyce, Senior Advisor of DataArt UK:
The single biggest security threat of 2016 will be the enemy within - companies' own staff.
Ian Kilpatrick, Chairman of Wick Hill Group:
It will be the untrained, uneducated, and just plain dumb users who put companies at risk by clicking bad links, visiting compromised web sites and using the same passwords for all log-ins.
Richard Blanford, Managing Director of Fordway:
The biggest security threat is now and will continue to be people - if they do not adhere to security policy and practice, whether through ignorance, carelessness or malicious intent, the best technology in the world will not prevent security breaches.
Ash Patel, Director of Business Transformation Cobweb Solutions:
Businesses of all sizes rely on the cloud for practically everything- and while they may purchase security services to protect against perceived threats managers forget that human error and internal misuse remains the biggest security threat to their business.
Andy Thomas, Managing Director, Europe, CSID:
Human fallibility - the one mistake or unknowing error that gives the bad guys access.
Corey Nachreiner, CTO of WatchGuard:
The single biggest threat you'll face in 2016 is your own people.
Richard Beck, head of cyber security at QA:
Whether as the result of malicious intent or genuine mistake, the actions of employees will be the single biggest threat to IT security in 2016.
Marie Bowman, Marketing Director at Digital Barriers:
Beware the insider threat, trusted individuals who already have privileged access to company assets will continue to be the single biggest security threat of 2016.
Bill Berutti, President of the Performance and Availability product line and president of the Cloud Management/Data Centre Automation product line for BMC Software, Inc.:
In 2016 the biggest security threat facing businesses is its own people.
Nick Pollard, UK General Manager of Guidance Software:
I think the biggest security threat of 2016 is the fact that cyberattacks are becoming ever more sophisticated and with that the ability to evade the security measures put in place to detect them, and what recent attacks have shown is that attackers today often use information gathered from people already on the inside – with this insider knowledge they can enhance the effectiveness of the attack and in certain instances make it utterly devastating.
David Gibson, VP of Strategy and Market Development at Varonis:
The single biggest security threat will be your employees – insiders – those that break bad, have their accounts stolen or blunder by clicking on links in phishing emails or putting sensitive data in the wrong place.
Clinton Karr, Senior Security Strategist at Bromium:
The biggest security threat is the endpoint; you can't patch users.
Rahul Kashyup, Chief Security Architect at Bromium:
The biggest threat for next year is YOU!
Jim Sneddon, Technical Director, at Aditinet:
The lack of properly trained cyber security educated people coming into the workplace along with poorly trained existing employees has been the #1 security flaw and source of breach for the last few years and investing in people will help secure your business for the future as well as now.

Data
Alex Raistrick, Director at Elastica:
With the SaaS and IaaS markets set to grow to $100 billion next year, the biggest security threat of 2016 will

be the lack of visibility of the vast amount of sensitive and personal 'shadow data' sitting in cloud applications, which is vulnerable to widespread data breeches and cyberattacks if not secured adequately.

Patrick Peterson, CEO and Founder of Agari:

Social Engineering - 2016 will be the year that criminals and nation states learn how to truly leverage their vast treasure troves of data about us, to craft attacks that trick us into wiring the funds, giving up our email passwords and installing malware ourselves.

Ron Hassanwalia, COO of SOTI:

Biggest security threat of 2016 would be shadow IT and data leakage.

Jes Breslaw, Director of Strategy at Delphix:

The biggest threat in 2016 will be the volume of insecure data sitting within IT infrastructure.

Gary Newe, Technical Director at F5 Networks:

The biggest security threat in 2016 will be to our personal data as a result of attacks on the browsers that we use to access the internet.

Justin Harvey, Chief Security Officer at Fidelis Cybersecurity:

The single biggest security threat of 2016 will be more legislation on data privacy and security.

Chris Merritt, VP of Product Marketing and Strategy for Blancco Technology Group:

As the exponential growth in data continues, legislative and regulatory pressure increases, and cybercrime against organizations and individuals runs rampant, there will be increased attention to data governance and the full lifecycle of information from creation to storage and use through to deletion.

Mike Turner, Global Cybersecurity Portfolio Head at Capgemini:

Citizen privacy and data confidentially breaches resulting from consumers and enterprises placing their trust in fundamentally insecure digital services.

New-fangled blackmail

Margee Abrams, Director of IT Security Services Product Marketing, Neustar:

New methods for old cons: Cybercriminals are using the old but tried and tested scams such as extortion and blackmail and repurposing them for the internet.

Cameron Brown, cyber expert:

Ransomware - the relative ease with which miscreants can disseminate ransomware, the high gains afforded to perpetrators, and the inability of law enforcement to counter this threat will ensure that motivation for development of new variants of this malware family remains strong in 2016 and beyond.

Elad Sharf, Security Research Manager at Performanta ltd:

I believe cyber extortion/ransomware will be the cyber security threat that causes the most impact in 2016 as, unlike traditional attacks which work slowly and aim to remain undetected, the impact of ransom based attacks is immediate, shocking and allows the perpetrators to profit directly by extorting funds.

David Kennerley, Threat Research Manager at Webroot:

Ransomware, the biggest threat of 2015 is going nowhere.

Josh Bressers, Security Product Manager at Red Hat:

I predict 2016 will see a dramatic rise in cyber extortion, such as ransomware, requiring payment to unlock important data and even threatening to publish sensitive corporate data if payment isn't made and CIOs should be factoring in a strategy now as to how they might deal with this.

Matt Walmsley, EMEA Marketing Director at Vectra Networks:

Commercially motivated targeted attacks leading to high profile data breaches, particularly from Eastern European sources.

IT, the laggard

Jeremy Bergsman, a Practice Leader at CEB:
Lack of "security hygiene" is the biggest threats companies are facing when it comes to IT, this is all the more important when research has shown that 99.9% of cyberattacks have exploited a flaw that has been present for over a year and never fixed, either due to a lack of training or because IT teams underestimated the potential severity of a minor flaw.
Dr Stephen Topliss, Head of Product at ThreatMetrix:
The biggest security threat for 2016 is the ineffectiveness of traditional methods of identity assessment.
Simon Crosby, CTO and Co-Founder, Bromium:
The biggest threat is poor IT practice, a laissez afire approach to patching and an assumption that AV still works.
Tad Johnson, Commercial Marketing Manager, JAMF Software:
I anticipate the biggest threat in 2016 will be vulnerabilities due to unmatched or outdated software.
Darin Welfare, EMEA Vice President at WinMagic:
Businesses must return to the fundamentals of security in 2016 because today's patchwork and piecemeal approach to data encryption exposes them to significant risk.
Gert-Jan Schenk, Vice President EMEA at Lookout:
CISOs and CIOs need to adopt smart security technologies that take advantage of security advancements like big data and machine learning to spot security issues before they become a problem.

Hacktivism and espionage
Leo Taddeo, Chief Security Officer at Cryptzone:
Without a doubt, Russian intelligence services and organised cybercriminals will continue to present the most serious cyber threat to US financial institutions, critical infrastructure, and sensitive government databases.
David Calder, Security Practice Director at ECS:
We'll see an increase in the sophistication of attacks as advanced techniques, developed by state-sponsored actors, become available to organised crime and terrorist organisations, resulting in further data breaches and potentially critical infrastructure impact.
Brian Kinch, Senior Partner in Fair Isaac Advisors:
The biggest single security threat is cyber - more specifically, for business and political entities it is probably nation state espionage and APT (advanced persistent threat) actors.
Thomas Fischer, Principal Threat Researcher, Digital Guardian:
Attacks such as those on TalkTalk and Ashley Madison have been blamed on the rise of 'hacktivism', which will undoubtedly continue in 2016 with increasing nationalism in countries like Russia and Syria acting as a major catalyst.
Jason Trost, VP of Threat Research at ThreatStream:
Transnational/Terrorist actors successfully targeting the power grid or oil and natural gas production, pipelines, etc., using a cyberattack with the goal of major disruption of service.
Rickey Gevers, Chief Intelligence Officer at RedSocks:
The single biggest security threat in 2016 will come from new and ever more sophisticated attack vectors, especially since the trend of nation state backed espionage has gone mainstream and exposing them has become like trophy hunting.

The Internet of Things
Phil Eyler, Executive Vice President and President, Infotainment from HARMAN:
Connected car solutions will need to be secure and 2016 will see a bigger emphasis with multi-layer security frameworks to ensure we keep systems safe.
Andrzej Kawalec, Global CTO for Enterprise Security Services at Hewlett Packard Enterprise:
In 2016 I see the Internet of Things as a new and rapidly expanding attack surface for adversaries to exploit.

Javvad Malik, Security Advocate at AlienVault:
Planes, guns, medical devices and automobiles have been hacked this year and vulnerabilities around the Internet of Things will continue to rise in 2016 as more and more internet connected devices are making their way into consumer hands.
John Hagerty, EMEA Director for Channels and Strategic Alliances at ForeScout Technologies:
The single biggest security threat of 2016 will be the Internet of Things (IoT): As predicted by Gartner, IoT will include about 26 billion units by 2020 and, during 2016, I predict we'll see a surprising increase in devices such as IP-connected smart TVs, DVRs, projectors and security cameras within the corporate environment, which are generally left out of the security sphere.
Tony Anscombe, **Senior Security Evangelist at AVG:**
The continued proliferation of devices in every home means that securing a single device is no longer an option.

Confusion from the wider business
Daniel Hedley, Associate at Thomas Eggar:
Sadly, I suspect that the single biggest threat to security in 2016 will be the same as it was in 2015; businesses continuing to make basic errors in their security arrangements, and continuing to starve their information security function of the resources they need to be effective.
Piers Wilson, Head of Product Management at Huntsman Security:
The biggest threat in 2016 will be those outside IT failing to understand the risks the business faces and continuing to underestimate their own responsibility in protecting their organisation.
Richard Olver, VP EMEA of Tanium:
The biggest threat is the language of IT and Cybersecurity organisations not being understood by the board, compounded by over 50% of boards lacking awareness; the ramifications of which on share prices, business revenues and brand equity are clear.
Chris Yule, Principal Security Consultant at Dell SecureWorks:
In 2016, demands on security experts will focus primarily on business priorities while also managing security risk as the growth of cyberattacks, combined with recent high profile victims such as TalkTalk and Sony, will help increase awareness of the dangers.

Specific threats
Michael Joerin, General Manager of EMEA at Namogoo:
The biggest security threat to retailers, banks, financial institutions and publishers in 2016 will undoubtedly be 'Client Side Injected Malware' – an insidious new form of malware which has grown rapidly in the past twelve months, infects one in three online users and enters the browser or device invisibly via unauthorised ads or spyware overlaid on top of genuine sites and made to look authentic – it cannot be blocked by traditional firewalls or anti-virus software.
Rohyt Belani, CEO of PhishMe Inc:
Phishing has been the #1 attack vector for 5+ years. 2016 will be no different as we, as an industry, are far behind the curve in our defences to combat email-borne threats.
Andy Harris, Chief Engineer at Osirium:
We see an increasing trend for phishing and stealing privileged credentials from the desktop, whilst brute forcing will wane.
Bharat Mistry, Cyber Security Consultant at Trend Micro:
Mobile malware will significant increase – the origins for these will be from emerging economies – such as India for example.

John Gunn, Vice President of Corporate Communications for *VASCO:*
We are already seeing a significant increase in attacks on mobile devices and mobile banking transactions, and this will certainly increase as criminal hacking organisations chase a bigger target.
Andrew Nanson CTO cyber at CORVID:
Malvertising is probably the most effective current method for large-scale compromise of hosts; where attackers buy advertising space on trusted websites and then embed code that runs on the victims' machines.

Other comments:
Chris Pace, Head of Product Marketing at Wallix:
2016 should be the year we stop categorising the difference between insider threats and externals attacks: the biggest challenge for the year ahead will be joining up traditional perimeter defences with better protection against attacks from the inside.
Kevin Burns, Head of Solution Architecture at Vodat International:
The biggest threat remains the internet; cybercrime is omnipresent and indiscriminate and all organisations need to defend with vigour and monitor with diligence.
James Chappell, CTO at Digital Shadows:
Criminals will continue to be relentless in their pursuit to steal, compromise or destroy business information including intellectual property.
Catalin Cosoi, Chief Security Strategist at Bitdefender:
In light of this year's recent events, it's safe to assume that some of the biggest threats for 2016 will have to do with the Internet of Things, ransomware (for both Windows and Linux), and an increase in data breaches.
Stephen Cox, Chief Security Architect at SecureAuth:
2016 will be the year of adaptive authentication.
Yorgen Edholm, CEO at Accellion:
Expect more national regulations and standards for privacy and international file-sharing.
Jeremiah Grossman, Founder, WhiteHat Security:
It's only a matter of time before the bad guys start exploiting the security software itself to compromise an organisation.
Shane Buckley, CEO, Xirrus:
Awareness of public Wi-Fi vulnerabilities is at an all-time high.
David Juitt, Chief Security Architect at Ipswitch:
New practices will be implemented to replace the Safe Harbour system - business will have to conduct a review of current procedures, pay close attention to the requirements of the EU data privacy law, the General Data Protection Regulation (GDPR), and assume that whatever comes next will be more rigorous and require an evidence trail.
Wieland Alge, VP & GM EMEA at Barracuda Networks:
Growing adoption of zero trust environments – if everything is put under the microscope then it makes it a lot harder for the hackers to make their way in and hide inside the network, the advanced nature of modern attacks means that you can't be too careful.
Ian Trump, Security Lead at LOGICnow:
Most businesses are going to need to be fully IPV6 to accommodate all of the devices that are going to be added to the network.
Roberto Casetta, Senior Vice President and General Manager, international at HEAT Software:
The biggest security threat of 2016 will be balancing productivity with heightened endpoint security across the increasingly borderless enterprise, a challenge that is driving the need for a layered defense-in-depth approach that proactively prevents infections.
Matt Middleton-Leal, Regional Director of UK and Ireland at CyberArk:
With 61% of respondents in our Threat Landscape report citing privileged account takeover as the most

difficult stage of a cyberattack to mitigate, and 38% saying that stolen privileged or administrative accounts were their greatest security concern, it's clear that the potential to compromise these powerful accounts – which hold the keys to the kingdom – is the greatest threat to security in 2016.

Mike Hickson the Managing Director of LSA Systems:

The biggest security threat for 2016 will be the move away from information driven hacking towards attacks on company infrastructure such as telecommunications and cloud based tools.

One more, this time from DataArt's NY MD, Alexei Miller:

The single biggest security threat of 2016 will be compromise.

Nick Braund, Head of Technology and Innovation at PHA Media:

Cyber security was a huge talking point this year, for the next 12 months the mere challenge of the next news-stopping hack, à la Ashley Madison, will again be prominent.

Andy Heather, VP EMEA, HPE Security at Data Security:

The threats and challenges will continue to grow exponentially, so trying to fix everything will fix nothing.

Professor Peter Cochrane OBE, futurologist and former CTO of BT:

If we do not up our security game, today's 'identity theft' epidemics will be rapidly eclipsed by 'ownership theft' on an even bigger scale.

Original article – http://www.idgconnect.com/abstract/10693/what-single-biggest-security-threat-2016