REDSCAN

ETHICAL HACKING IN 2020:

Risks, Challenges and Trends




redscan.com

1. Dispelling the stereotypes around ethical hacking

The hoodie – that's the stereotypical image which comes to mind when people hear the word hacker, even if it's in relation to cyber security professionals. The perception is that hackers work in dimly-lit bedrooms on the fringes of society looking to cause damage and destruction.

Mainstream media coverage often perpetuates the stereotype, and, for this reason, many people remain sceptical about hacking. They may believe that it hinders rather than helps the security of organisations.

Over the last 12 months, there has been an unprecedented number of security breaches. As a result, coverage of hacking in the national media has cast it in a poor light, focusing on the negatives rather than the many positives.

2. Ethical Hacking Roundtable 2020

As a counterbalance to misconceptions about ethical hacking, Redscan decided to bring together a number of industry experts to consider the state of the industry and examine current risks, challenges and trends.

The panel discussed what constitutes 'ethical' in the context of hacking; the benefits of hacking to businesses and society; where the boundary lies between legal and illegal activity; and other hot topics for 2020.

Mark Nicholls
CTO, Redscan

Anthony Lee
Partner, Rosenblatt Limited

Giles Ashton-Roberts
CISO, FirstGroup

Ian Glover
President, CREST

Jake Davis
Security Consultant and former Lulzsec hacker

Jim Hart
CISO, Pollinate International

Lauri Love
Security Consultant and British hacktivist

Raef Meeuwisse
Author and ISACA Speaker

Disclaimer: All views expressed at the Ethical Hacking Roundtable 2020 are those of the individual and do not necessarily reflect those of Redscan.

3. What is ethical hacking?

To open the discussion, our panellists considered what distinguishes an ethical hacker from a hacker, or if there even is a distinction between the two.

Mark Nicholls Redscan
"From my perspective, an ethical hacker is someone who has an attacker's mindset, but they have full permission to be doing the hacking. It is a benefit for the client and for society more generally. If the hacker doesn't have express permission, then it's unethical."

Jim Hart Pollinate International
"I'd actually make the definition a bit broader; as well as someone carrying out pen testing, I would include someone who doesn't have permission, but who is looking for vulnerabilities in IT systems. They are not necessarily getting payment, but the hacker may be uncovering liabilities, in order to report them rather than exploit them. Whilst this may not necessarily be legal, I would consider it ethical still."

Ian Glover CREST
"I find the term ethical hacking a contradiction and it is not one I like to use. Instead I use a more descriptive term such as penetration testing and intelligence-led penetration testing for red teaming. The term hacker has a certain connotation in the marketplace, so I prefer to use alternatives."

Jake Davis
"I would take an even broader definition of what an ethical hacker is; I agree with Ian that it is a redundant term, but that's because I believe all hacking is ethical. There is still a stigma – I just say hacker and I enjoy saying hacker. I would include criminal hacking in this too, as it depends on whose law is being applied."

Lauri Love
"I agree, I'm not a former hacker, just a continuing hacker who is on the right side of the law. Being a hacker is a mindset, it's about taking things apart. I see ethical hacking as when you are in a symbiotic relationship with whatever you are hacking; you need to look at what the parameters are, what is the trust, and have an agreement to not cause damage whilst undertaking the hacking."

Key factors that help to determine whether hacking is ethical:

- Intent
- Consent
- Scope
- Methodology
- Legality
- Rules of engagement
- Outcomes
- Trust

"I like to use a more descriptive term such as penetration testing"
Ian Glover, CREST

"All hacking is ethical"
Jake Davis

"Being a hacker is a mindset, it's about taking things apart"
Lauri Love

4. What are the benefits of ethical hacking?

The panellists then discussed what they saw as the benefits of ethical services, such as penetration testing and red teaming. The panellists highlighted how ethical hacking helps organisations to improve their security posture, comply with industry and national regulations, and reduce the overall risk of falling victim to cybercrime.

Mark Nicholls Redscan
"In ethical hacking, the value add for a client is learning where your security controls sit and whether they are effective. Protecting data benefits not only an organisation but their customers and wider society too."

Giles Ashton-Roberts FirstGroup 
"As a transport provider, we follow the NIS Directive, as well as a requirement to protect consumer data under the likes of GDPR and PCI DSS, so we are torn all over place. We use ethical hacking as a continual improvement programme, with a series of pen tests carried out through the year. For me it's not just a tick box exercise. It's about making the improvements, closing the gaps on the vulnerabilities that are found."

Jim Hart Pollinate International
"I work in a different industry, in the financial tech sector, but we take a similar approach to Giles. Whether the outcome is good, bad or ugly, at the end of pen test for compliance terms, the crucial part is the validation of our delivery methodology. We are looking not just at the remediation of the vulnerabilities found, but also for the root causes, so these can be addressed too."

Ian Glover CREST 
"The word 'test' has the connotation of a pass but that's not possible with pen testing. Instead it is about providing assurance in a fast-changing technological world. Regulators are now being more involved as cyber gets board-level attention, so we need to improve security not just by testing but by giving clients actionable outcomes."

Lauri Love
"I agree there is a move for the hacker to be more integrated with the client, not just testing. This enables the hacker to give clients a better understanding of their systems as they continuously evolve in their search for the unobtainable perfection of security of their systems. This relationship builds a rich eco-system in the industry with threat hunting, sharing information online together and a rising professionalisation."

Key benefits:

- Fixing vulnerabilities before they are exploited by cybercriminals
- Providing independent assurance of security controls
- Improving awareness and understanding of cyber security risks
- Supporting PCI DSS, ISO 27001 and GDPR compliance
- Demonstrating a continuous commitment to security
- Supplying the insight needed to prioritise future investments

"For me it's not just a tick box exercise but it's about making the improvements, closing the gaps on the vulnerabilities that are found"
Giles Ashton-Roberts, FirstGroup

"We need to improve security – not just by testing but by giving clients actionable outcomes"
Ian Glover, CREST

5. Challenges for 2020

The panel of experts identified six key challenges for 2020 faced by businesses and individuals working in the security industry:

1. Staying on the right side of the law
2. Overcoming organisational resistance
3. Coping with the skills shortage
4. Creating appropriate pathways for hackers
5. Keeping up with digital transformation
6. Showing the value of ethical hacking

5.1 Staying on the right side of the law

The issue suggested by the panel as arguably the biggest challenge for the industry in 2020 was ensuring that ethical hacking stays on the right side of the law. This is important for maintaining the integrity of organisations, the rights of their customers and for safeguarding security professionals themselves.

This was highlighted recently when employees of a penetration testing company in the US state of Iowa were arrested for carrying out a legally contracted assignment to pen test systems.

Anthony Lee Rosenblatt Limited
"There are several laws out there that demand ethical hacking, such as the NIS Directive for operators of essential infrastructure and cloud services; financial services regulations; then of course there is GDPR.

"Whilst GDPR encourages the use of ethical hacking as an appropriate security measure, you also have to carry out the ethical hacking in such a way that it doesn't itself fall foul of the law. This could happen by the disclosure of personal data to ethical hackers as they undertake the testing. An analogy is that you can open the safe, but you can't look at the contents."

Jake Davis

"Ideally as a hacker, you would want to open the safe and look at the contents. If you can't emulate a real hacker, then you get boxed in and you can't do your job. The scope of what you can test in the UK can be tricky, but it is getting better.

"Often, it's a case of saying you have never seen the contents, then signing a lot of documents to say you've not seen the contents. And in more extreme scenarios, sign a document to say that you can't even replicate those contents in any shape."

Key takeaways:

- Understand which legal frameworks apply
- Seek qualified legal advice
- Have a strong contract in place
- Use accredited suppliers
- Treat suppliers as temporary employees to provide access to data

CONTINUED

5.1 Staying on the right side of the law

Anthony Lee Rosenblatt Limited
"It gets even more difficult when you have sensitive personal data in the mix, as there is no lawful basis for processing that data in penetration testing, so you run into difficulties there."

Lauri Love
"As an attacker, you leverage pieces of personal data to get deeper into a system and find out more, so there are inherent tensions in the system. As a company, you want to bring someone in you can treat like an employee. You don't want downtime or any leaks of confidentiality, but you do want people who simulate real-world attackers as closely as possible and they, of course, don't have to follow these rules."

Ian Glover CREST
"To help tackle this, some companies are extending their acceptable use policies to include ethical hacking companies."

Lauri Love
"Alternatively, testers can sometimes be indemnified as temporary employees. But potentially, we need to create a new class of citizen for ethical hackers. People with special powers to process data, similar to the powers that the National Crime Agency Specials have."

Anthony Lee Rosenblatt Limited
"When a company is bringing in a third party to do penetration testing then they need a strong contract. Clients are quite cautious when they bring in pen testers, so they look for companies with accreditation; a good reputation; how they comply with the law for GDPR when data is exposed."

Ian Glover CREST
"Even if you are an intelligent buyer, it is hard to put together an invitation to tender that replicates a contract and the level of assurance you should have in place. At CREST, we operate as though we are the hardest ITT (Invitation to Tender) that any supplier will ever face, and this then offers those levels of assurance to buyers of penetration testing."

"In the context of GDPR as an ethical hacker, the analogy is you can open the safe, but you can't look at the contents."
Anthony Lee, Rosenblatt Limited

"If you can't emulate a real hacker, then you get boxed in and you can't do your job."
Jake Davis

"Potentially we need to create a new class of citizen for ethical hacking who are able to have special powers to process data"
Lauri Love

5.2 Overcoming organisational resistance

Another strong theme from the panel discussion was that not all organisations have historically been willing to embrace ethical hacking – not because they don't appreciate its value but because they feel that hackers could cause embarrassment or even increase workload. However, there are signs of change.

Mark Nicholls Redscan
"I feel that in the past there has definitely been an embarrassment or fear factor for some organisations in engaging ethical hackers".

Jim Hart Pollinate International 
"There shouldn't be a fear factor. There's no such thing as 100% security, you will be attacked, it's an inevitability. So, I think that once you understand that, it changes the way you look at ethical hacking".

Mark Nicholls Redscan
"Several years ago, I was doing penetration testing into Tier One banks but none of them wanted to be the first to open themselves up for scrutiny. But as time went on, the banks became willing to invite ethical hackers in to compromise their systems and sensitive operations. They were looking for assurance that any exploits wouldn't bring down their system. I think that transparency really helped allay those fears."

Raef Meeuwisse ISACA 
"There aren't any good arguments against carrying out ethical hacking. However, it is my experience that lots of organisations have badly under-resourced security teams. The problem is that as they are already overstretched. They often know that they are sitting on a load of risks already, so they don't want a bunch of ethical hackers to come and tell them about more."

Lauri Love
"So it's a case of ignorance is bliss."

"I find that the most useful pen tests are the ones where you don't pass, when something comes up. If nothing comes up, then as the client you feel protected but that may not be the truth. When you can turn something being found into a win, then that's when the underlying processes gets changed and everyone is actually winning."

Key reasons for resistance identified:

- The fear or embarrassment factor
- Not enough resources to undertake testing in-house
- Ethical hacking viewed as creating more new work
- Possible operational disruption

"You will be attacked, it's an inevitability. Once you understand that, it changes the way you look at ethical hacking"
Jim Hart, Pollinate International

"Transparency has really helped allay the fears of organisations in engaging ethical hackers"
Mark Nicholls, Redscan

5.3 Coping with the skills shortage

Another strong theme from the panel discussion was that not all organisations have historically been willing to embrace ethical hacking – not because they don't appreciate its value but because they feel that hackers could cause embarrassment or even increase workload. However, there are signs of change.

Raef Meeuwisse ISACA
"At ISACA, we've just completed a survey that looked at the technology landscape for the 2020s. One of the key responses from the 5,000 security professionals surveyed was that 81% of them didn't feel that their organisations were investing enough in people skills to be prepared for the threats of the next decade."

Mark Nicholls Redscan
"I have seen issues with some people coming into the industry recently. Those with certain certifications and those individuals that are fresh out of university, they just don't have the practical experience. Maybe there isn't the right level of exposure in university, so we have to find a way to create better hackers."

Ian Glover CREST
"In terms of trying to find new talent in the marketplace, there are some exceptional people who have come into the industry with a background of working in technical architecture or in technical testing. And those people are an example of the type of skillset that would be really good to try and introduce into the marketplace."

Mark Nicholls Redscan
"There's also a need for more specialist testers too in certain areas, such as cloud security."

Lauri Love
"We have such a shortage of pen testers that we need to open up the industry more to bug bounty hunters. Some companies have such a large attack surface that they can't possibly hire enough security professionals to protect the organisation.

"So, you open it up to the world – but this is an entirely different threat model. Because it is open ended, these people, by definition, cannot be assessed or have the accreditations."

Ian Glover CREST
"You're right, we want to bring in elements of those people doing ethical hacking, people who are experimenting with things. We want to bring them into the industry in a controlled way and we need to think about how that operates."

Key takeaways:

- Value and invest in your existing employees
- Consider bringing in competent individuals from other disciplines
- Blend the skills of bug bounty hunters with qualified security professionals

"81% of organisations are not investing enough in people skills"
Raef Meeuwisse, ISACA

"There is a need for more specialist testers in certain areas, such as cloud security"
Mark Nicholls, Redscan

5.4 Creating appropriate pathways for hackers

The panellists also discussed the importance of encouraging people onto the right pathway so that they didn't get drawn into the darker side of hacking.

Lauri Love
"We need to understand what motivates hackers – it's fun, it's exhilarating, breaking into systems. It can also be very profitable selling that information on to organised crime, nation state actors, or even industrial competitors who might want to play dirty."

Jim Hart Pollinate International
"We know that we're going to be attacked, so let's incentivise people to report what they find."

Lauri Love
"Through bug bounty brokers there is this swarming hive of curious, bored people out there who are attacking things and occasionally striking gold. We need to create the right incentives for them to report to companies rather than make more money elsewhere through malicious activity. Ideally, it should also be more fun too."

Ian Glover CREST
"We also need to think about how we protect vulnerable young people. It is difficult, people are inquisitive. We are seeing an increasing amount of grooming where vulnerable young people are going through gaming into mods, into extraction tools, into hacking forums. So, we need to have a process that will help to re-socialise them."

Jake Davis
"Young, would-be hackers want respect and not to be patronised. I think it's great to see the National Cyber Crime Unit is no longer using the Computing Misuse Act for what I would call trivial acts: for example, if a gamer gets annoyed at losing online, and then they decide, in frustration, to go after the games company with a denial of service attack."

Ian Glover CREST
"I think law enforcement in the UK is leading the way globally, with our thought leadership over the last four years in identifying vulnerable young people. Feedback from parents has been good, saying that often this is the first time that someone has had a proper conversation with their child about their skills and potential."

Lauri Love
"Kids get bored in school and they end up knowing more than their teachers, so they develop skills in an uncontrolled manner. I'd like to see them learning hacking, development and programming in more of a youth club or sports centre style. And that we get engagement with industry representatives like CREST, or with companies like Redscan, to work with this burgeoning talent to get the most out of them."

Key takeaways:

- Alter the way children are taught IT
- Continue to build bridges between industry and the hacking community
- Create the right incentives for responsible disclosure
- Develop new ways to engage rogue hackers

"We also need to think about how we protect vulnerable young people"
Ian Glover, CREST

"I'd like to see kids learning hacking and programming in more of a youth club or sports centre style"
Lauri Love

5.5 Keeping up with digital transformation

We all know that technology never stands still, and the panel explored areas of technological advances in ethical hacking that stand to impact the industry most within the next 12 months.

Mark Nicholls Redscan
"The industry is only going to grow. We keep on seeing massive breaches all the time. Only the other week there were 1.2bn records found on the web as organisations continue to move to the cloud.

"Generally, the complexities and configurations of those cloud environments are still not well understood, so you see the problems we're having with data leakage. The traditional toolset for detecting and monitoring those environments is a challenge. We need to see an improvement in tools such as serverless Docker and Kubernetes, as the tool set isn't there yet."

Ian Glover CREST
"We now have some young people with complicated extractive tools that can do quite a lot of damage. They have access to illegal bits of software that come with in-built extraction capabilities and ransomware."

Raef Meeuwisse ISACA
"We also need to think about machine learning and artificial intelligence, and how these can be put to use, including by hackers. So, the trajectory we are on at the moment is that a lone individual working in a bedroom can potentially take out the national infrastructure of an entire nation. Unless we use tools like ethical hacking to understand where the technological risks are, the vulnerabilities are quite extreme."

Anthony Lee Rosenblatt Limited
"Legally, there are grey areas around machine learning, artificial intelligence and the automation of personal data. There are challenges around these topics, and we don't have all the answers to the questions at the moment."

Lauri Love
"The consequences of machine learning aren't always what were intended. We've seen examples such as how a piece of software the police were using in the US learnt how to be racist, as it picked out suspects based on skin colour. We need to be careful how biases affect the tools we are using and developing.

"It's the same in algorithms, for example where bots have hijacked the discourse on social media tools like Facebook and Twitter to push a particular agenda, including to disrupt politics in both the UK and the US."

Key takeaways:

- Understand that the legal aspects of some new technologies are unclear
- Be aware of the power of software that can be used for malicious purposes
- Engage with specialists when dealing with cloud security

"The complexities and configurations of cloud environments are still not well understood"
Mark Nicholls, Redscan

"A lone individual can potentially take out the national infrastructure of an entire nation"
Raef Meeuwisse, ISACA

5.6 Showing the value of ethical hacking

Another challenge the panellists discussed was the problem that many organisations face in securing appropriate investment to invest in ethical hacking. A common occurrence the panellists also identified is in failing to secure enough budget to handle the cost of remediation.

Raef Meeuwisse ISACA
"It feels like we are entering a new era now, where organisations that are not taking their cyber security seriously will not survive. If you look at cybercrime revenues versus cyber security investment there is a clear mis-match.

"In 2017, there was $1.5 trillion lost in cybercrime and unexpected outages, whilst at same time the spend on cyber security was $15bn, which is only 10% of the cost. And that gap is widening as cybercrime is doubling, but investment is only going up by 10 to 15% a year - it's just not keeping pace."

Giles Ashton-Roberts FirstGroup
"It is crucial to make sure that boards understand the situation. I never say to my board that we are secure, as the threats are always changing, but that we are always trying our best to make us as secure as possible. By doing this we are continually improving, and so we are looking after our reputation."

Jim Hart Pollinate International
"You can make the argument to a board that the cost of a pen test is offset by the fact that you don't have to remediate as much in the future. If you can demonstrate cost savings to the board, that's when you get buy-in from them."

Lauri Love
"I explain this to a board as technical debt. You pay a significantly lower cost by tackling an issue, than if that problem gets pulled out into the wild."

Mark Nicholls Redscan
"Whilst many organisations are still not open to penetration testing, I do see some businesses becoming more open. I see increasing amounts of senior executives who are more open and engaged to penetration testing, and even willing to let themselves and their C-Level team be phished to try and extract money."

Ian Glover CREST
"Although businesses are paying money for ethical hacking, they are not putting the money aside to deal with the triage and the remediation of the findings."

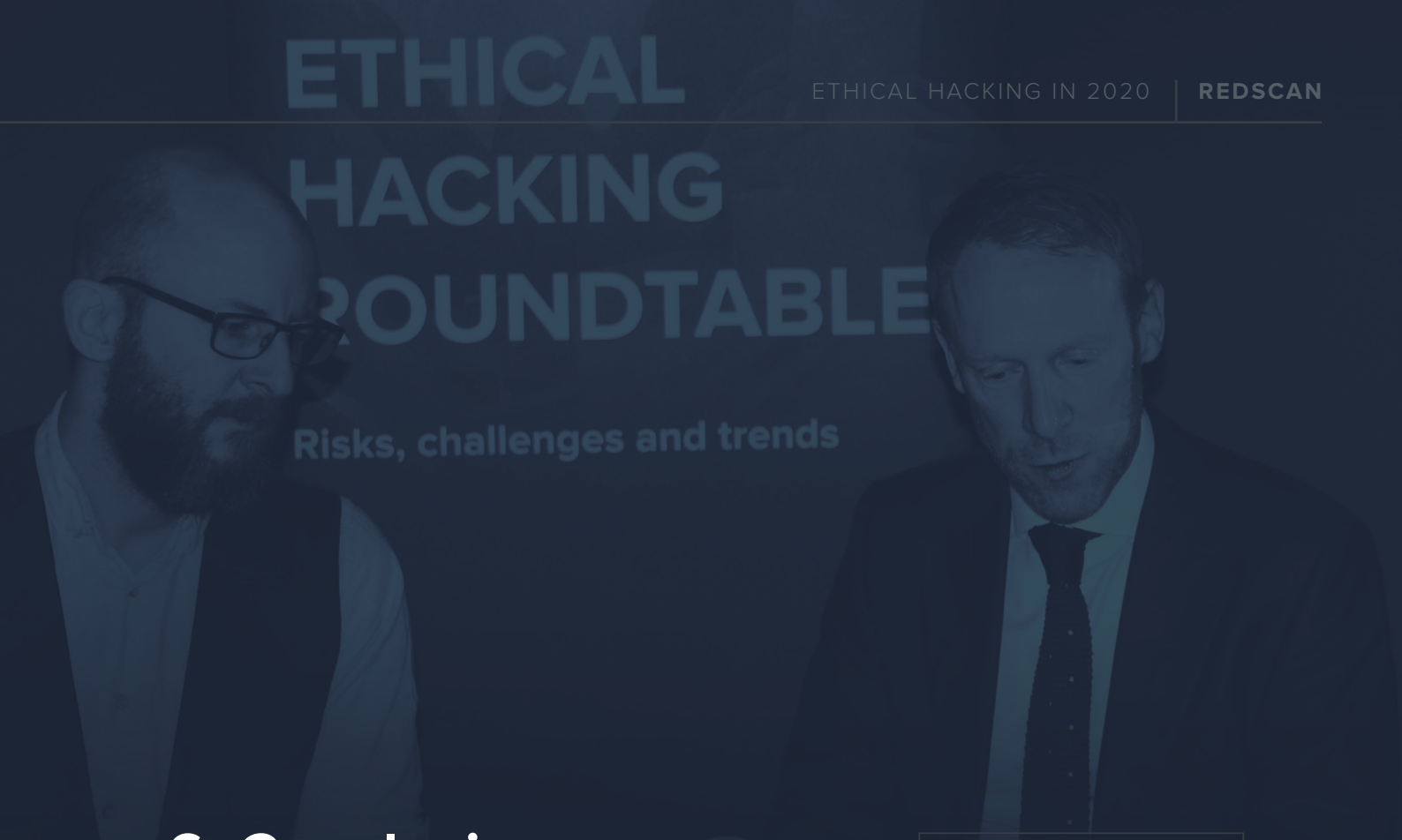
Giles Ashton-Roberts FirstGroup
"You definitely need to set funds aside to make sure that the findings of penetration testing are reviewed and acted upon. If not, you are wasting money by doing the penetration testing."

Key takeaways:

- Ensure that boards understand the value of ethical hacking
- Increase expenditure on ethical hacking to keep up with the rising threat
- Budget for doing remediation work on the findings of testing
- Gain acceptance for ethical hacking across the C-suite

"Organisations that are not taking their cyber security seriously will not survive!"
Raef Meeuwisse, ISACA

"If you are not setting funds aside for remediation, you are wasting money by doing the penetration testing"
Giles Ashton-Roberts, FirstGroup



6. Conclusions

The view from the 2020 Ethical Hacking Roundtable, hosted by Redscan, is that whilst there are still many myths and stereotypes around ethical hacking, its value is now beginning to gain mainstream recognition. This is evidenced by the gradual shift in the perception of hacking and the increasing adoption of cyber security measures by businesses.

The roundtable panellists agreed that organisations need to be prepared to invest in defending effectively against cybercrime and to nurture the skills that will enable them to protect themselves. They also highlighted the need to develop pathways for ethical hackers of the future and to consider how approaches must evolve in line with new technologies and regulations.

While the challenges for ethical hackers are varied, so too are the opportunities to play a vital part in protecting the status and the success of organisations.

> *"Things are moving forward positively in hacker culture, which is a nice thing to say!"*
>
> Jake Davis

> *"We've come a long way as an industry, we've leap-frogged over not just the cyber industry but also the IT industry too"*
>
> Ian Glover, CREST

> *"In 2020, more organisations will realise the benefits of ethical hacking"*
>
> Mark Nicholls, Redscan

Ethical Hacking Roundtable 2020 Panellists

Mark Nicholls
CTO, Redscan

Mark has been working in the cyber security industry for over 11 years and in this time has quickly established himself as a leading information security professional within the UK security market. He was recently awarded a CREST Fellowship.

Watch the interview with Mark

Anthony Lee
Partner, Rosenblatt Limited

Anthony is a partner and commercial lawyer with more than 25 years' experience of advising clients on the legal issues surrounding the deployment and use of established and disruptive information technology.

Watch the interview with Anthony

Giles Ashton-Roberts
CISO, FirstGroup

For the last five years, Giles has been driving technological change at FirstGroup, most recently in the role of Chief Information Security Officer. FirstGroup is a leading provider of transport services in the UK and North America.

Watch the interview with Giles

Ian Glover
President, CREST

Ian has been working in information security for the last 38 years. As President of CREST, he has been instrumental in a significant number of major initiatives in the cyber security industry, including the Cyber Essentials, STAR and CBEST schemes.

Watch the interview with Ian

Jake Davis
Security Consultant and former Lulzsec hacker

Ex-Lulzsec and Anonymous member, Jake Davis (aka Topiary) is an experienced security speaker, consultant and author. He is interested in the psychology and emotional complexity behind cyber security and is working to educate and inform the next generation(s) of technology experts.

Watch the interview with Jake

Jim Hart
CISO, Pollinate International

Jim has over two decades of experience in developing security strategy and working with technology partners to protect business assets and people from cyber-attacks.
He has recently created a diverse security function at Pollinate International Limited in the fintech sector.

Lauri Love
Security Consultant and British hacktivist

Lauri is a British-Finnish technologist and political activist. In 2018, he won a landmark legal appeal against extradition to the USA, where he was facing prison for alleged involvement in an Anonymous hacktivist campaign. Lauri now works as a Security Consultant and continues to fight for privacy and civil rights in the digital domain.

Watch the interview with Lauri

Stephen Pritchard
Chair of the Panel

Stephen is a video journalist, broadcaster and writer. He is a contributing editor and columnist for IT Pro and for Infosecurity Magazine. Stephen also writes for a number of newspapers, including the Financial Times, the Guardian and Sunday Times.

Raef Meeuwisse
Author and ISACA Speaker

Raef holds multiple certifications for information security and is the author of many books on the topics of cybersecurity and social engineering, including the international best seller Cybersecurity for Beginners. Raef is also an expert speaker for ISACA, the international not-for-profit security organisation.

Watch the interview with Raef

REDSCAN

About Redscan

Redscan is an award-winning provider of managed security services, specialising in threat detection and integrated response.

Possessing a deep knowledge of offensive security, Redscan's experts are among the most qualified in the industry, working as an extension of clients' in-house resources to expose and address vulnerabilities plus swiftly identify and shut down breaches. Services offered include CREST accredited Penetration Testing, Red Teaming and Managed Detection & Response.

By understanding how attackers operate, leveraging cutting-edge threat intelligence, and offering highly acclaimed customer service, Redscan's cyber security professionals can be trusted to provide the insight and support needed to successfully mitigate information security risk and achieve compliance standards.

CREST

SC 2018 awards EUROPE Winner BEST CUSTOMER SERVICE

2019 Computing Security Awards WINNER

Cyber Security Awards Winner 2019

Call us
0800 107 6098

Email us
info@redscan.com

Twitter
@redscan

LinkedIn
/redscan