

Role of Cyber Security for Combatting Corruption



Prepared & Presented by:

Roland Abi Najem – CEO of Revotips

www.rolandabinajem.com



@rolandanajem



@rolandabinajem



@rolandabinajem



rolandabinajemofficial



RolandAbiNajem

Cyber Security Facts Stats

95% of cybersecurity breaches are due to human error

There is a hacker attack every 39 seconds

Since COVID-19, the US FBI reported a 300% increase in reported cybercrimes

Cyber Security Facts Stats

Human intelligence and comprehension is the best defense against phishing attacks

Connected IoT devices will reach 75 billion by 2025

Unfilled cybersecurity jobs worldwide is already over 3.5 million

Most companies take nearly 6 months to detect a data breach, even major ones



THE CYBERSECURITY SKILLS GAP

Why is education is our best weapon
against cybercrime?



Cybersecurity Jobs Report: 3.5 Million Openings In 2025

- The number of unfilled cybersecurity jobs grew by 350 percent, from one million positions in 2013 to 3.5 million in 2021. For the first time in a decade, the cybersecurity skills gap is leveling off. Looking five years ahead, we predict the same number of openings in 2025

Ref:

<https://www.einpresswire.com/article/556075599/cybersecurity-jobs-report-3-5-million-openings-through-2025>


Empowering Security Researchers Will Improve Global Cybersecurity

One of the most popular short- to medium-term solutions to combat this deficit is participating in Bug Bounty Programs (BBPs).

BBPs offer security researchers, also sometimes dubbed 'white hat hackers', a reward or bounty for finding and reporting vulnerabilities in software products.



Political Pressures and Regulatory Patchworks

- Although ethical hackers help to improve cyber defenses, their activities are often hampered by institutional deficits, legal uncertainties, or even political threats.
- 

Understand
Hackers &
Let Them
Help You

WHY DO HACKERS HACK?

85%

To Learn

76%

To Make Money

65%

To Have Fun

62%

To Advance Their Career

47%

To Protect & Defend
Businesses and Individuals

Hackers Report 2021 – Key Findings



63%

increase in the number of hackers submitting vulnerabilities over the past 12 months.



20

the average number of vulnerability categories top hackers report across.



53%

rise in submissions for Improper Access Control and Privilege Escalation.



310%

increase in reports for Misconfiguration.



50%

of hackers have not reported a bug because of a lack of a clear reporting process or a previous negative experience.

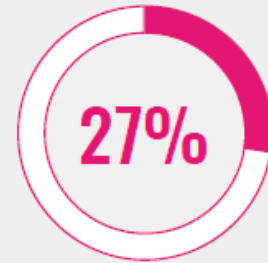


85%

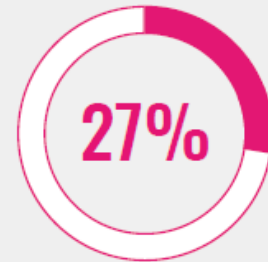
of hackers hack to learn and **62%** do it to advance their career.

Help Hackers Disclose The Bugs They Found

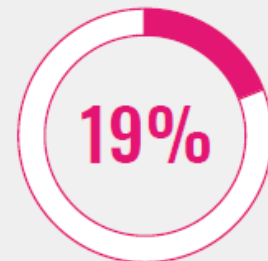
50% OF HACKERS HAVE NOT
DISCLOSED A BUG THEY FOUND.



Failed to report a bug because there was no channel through which to disclose it.

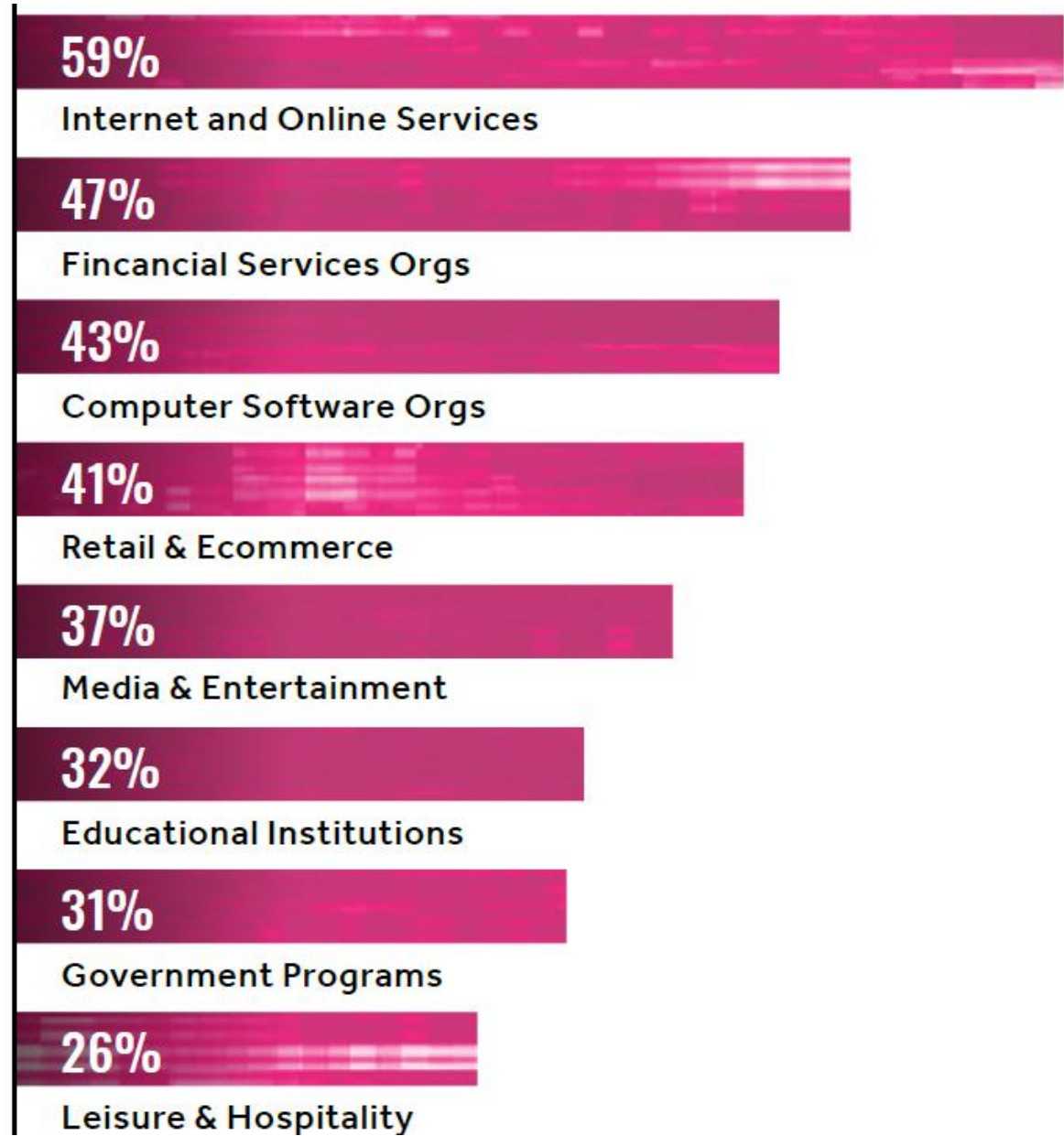


Failed to report a bug because the company had previously been unresponsive or difficult to work with.



Failed to report a bug because no bounty was offered.

Which Industries Are Hackers Working With?

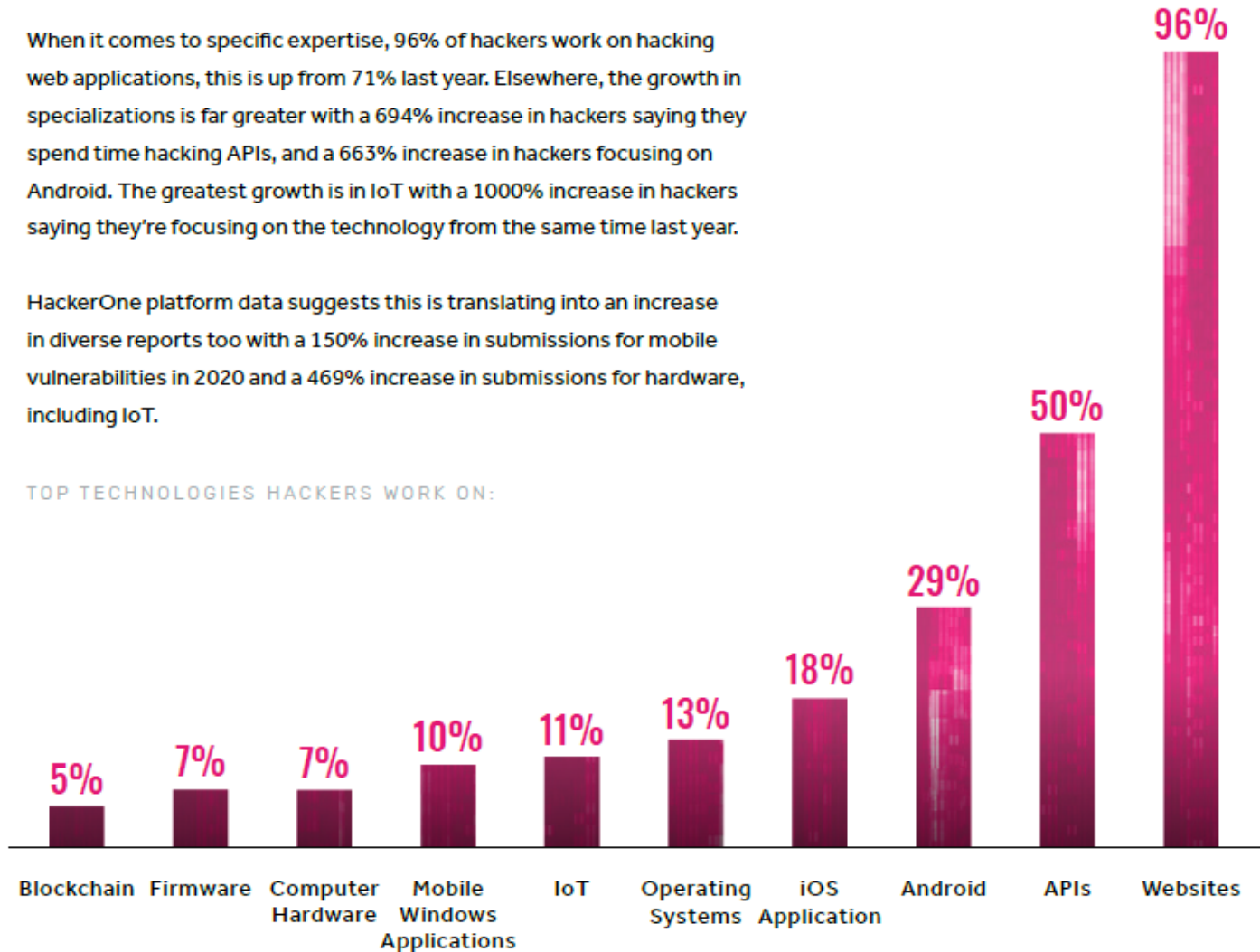


WHAT TECHNOLOGIES ARE HACKERS WORKING ON?

When it comes to specific expertise, 96% of hackers work on hacking web applications, this is up from 71% last year. Elsewhere, the growth in specializations is far greater with a 694% increase in hackers saying they spend time hacking APIs, and a 663% increase in hackers focusing on Android. The greatest growth is in IoT with a 1000% increase in hackers saying they're focusing on the technology from the same time last year.

HackerOne platform data suggests this is translating into an increase in diverse reports too with a 150% increase in submissions for mobile vulnerabilities in 2020 and a 469% increase in submissions for hardware, including IoT.

TOP TECHNOLOGIES HACKERS WORK ON:



The 2022 Attack Resistance Report – Key Findings

Only 1/3 Services or applications are tested and assessed more often than once a year.

66% Believe their teams lack excellent security skills.

Contributors to the increasing cyberattack surface

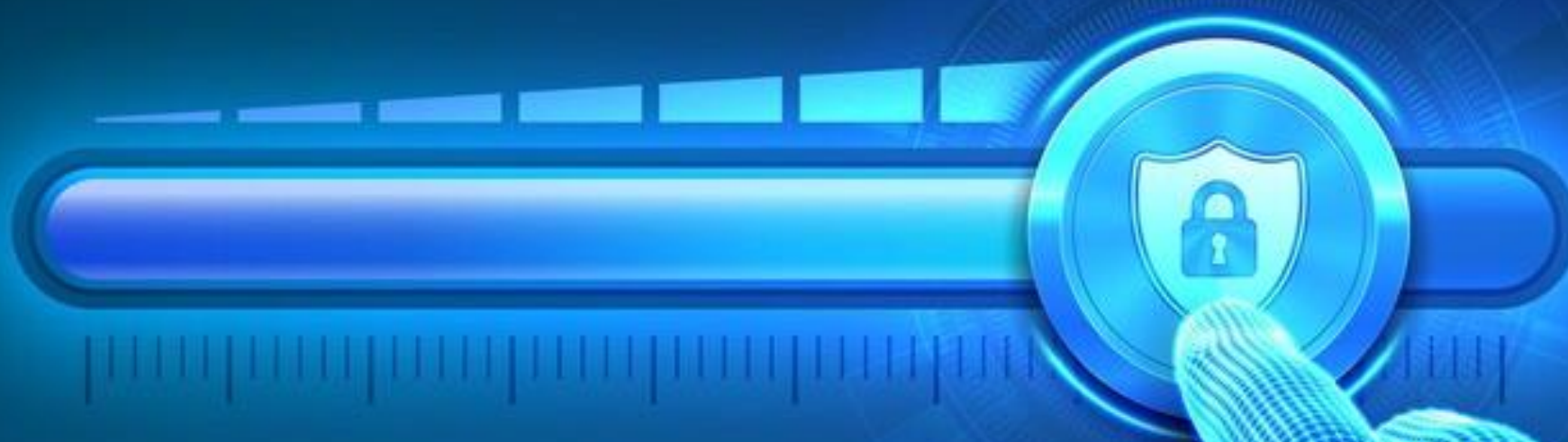
Cloud Adoption: A Harvard Business Review Analytic found that more than 60% of their IT portfolio will reside in the cloud within two years.

Work-From-Anywhere Model: An Upwork study projects that 73% of all teams will have remote workers by 2028.

Internet of Things (IoT) growth: According to IDC, 55.9 billion connected devices will be connected by 2025.

Before Attack Resistance Management	With Attack Resistance Management
<ul style="list-style-type: none">▪ Incomplete knowledge of the attack surface with unknown risks.	<ul style="list-style-type: none">▪ Improved knowledge of attack surface assets, prioritized by risk.
<ul style="list-style-type: none">▪ Insufficient pentesting and security assessments that are outnumbered by code updates.	<ul style="list-style-type: none">▪ Pentesting and security assessments are on-demand, accessible directly by development teams.
<ul style="list-style-type: none">▪ Scanning tools provide basic reports of known vulnerabilities, with high false-positive rates and an overabundance of information that is not easily actionable.	<ul style="list-style-type: none">▪ Security testing with a community of hackers provides more high criticality vulnerabilities and a lower volume of reports.
<ul style="list-style-type: none">▪ Lack of skills needed to test applications written and deployed in mixed environments.	<ul style="list-style-type: none">▪ On-demand hacker talent with almost any set of skills required.
<ul style="list-style-type: none">▪ Broken processes from monitoring to development to testing. Developer teams cannot learn from code scans.	<ul style="list-style-type: none">▪ Developers learn from vulnerability reports, reducing repetition of mistakes in the codebase and improving DevSecOps collaboration.

MIN



MAX

**ENHANCE
SECURITY LEVEL**

Don't Let Perfection be the Enemy of Better Than Before

Role of Cyber Security for Combatting Corruption



Thank You

Roland Abi Najem – CEO of Revotips

www.rolandabinajem.com



@rolandanajem



@rolandabinajem



@rolandabinajem



rolandabinajemofficial



RolandAbiNajem