11 EXPERT TIPS FOR YOUNG TECH EXECS RECOVERING FROM A DEVASTATING HACK

Published by Forbes | Comments by Forbes Technology Council


Forbes

Dec 1, 2020, 08:10am EST | 372 views

11 Expert Tips For Young Tech Execs Recovering From A Devastating Hack

Expert Panel® Forbes Councils Member
Forbes Technology Council COUNCIL POST | Membership (fee-based)
Innovation

Dealing with a major systems hack doesn't just mean addressing the present problem; it also requires building better protections so it's less likely to happen again. This can be especially challenging for young tech executives with minimal experience troubleshooting, diagnosing and revamping vulnerable systems.

The seasoned tech leaders of Forbes Technology Council have experience both in overcoming hacks and taking important steps to improve security. Below, they offer actionable tips to help new tech execs recover from a hack and shore up their defenses.

1. Minimise platform complexity.

Take steps to reduce future platform complexity to better identify areas of risk. Whether it's systems, networking or software architecture, the more complex the system, the harder it is to secure. If you implement a more modular design and reduce the number of tools, libraries and languages being used, there is less opportunity for vulnerabilities to get introduced. **Chris Sullivan, Castellum.AI**

2. Construct a comprehensive security framework.

The approach should be about building and adopting a companywide security framework. This involves people (improving skill sets and awareness, limiting access privileges and conducting training), processes (developing and enforcing policies, implementing monitoring, and conducting periodic assessments of enforcement) and systems (adding alerts, monitoring and defensive tools). Adopting a comprehensive framework can go a long way. **Vilas Uchil, BullsEye Telecom**

3. Build proactive security controls.

Create an integrated platform that ties together risk, security, compliance and software development. One approach is using balanced development automation to achieve defensible security assurance in a way that makes sense in business terms—namely, risk and compliance. The goal is to strike the right balance between security assurance and business speed. **Altaz Valani, Security Compass**

4. Hire an expert to review your situation.

Most infiltrations today are preventable by relatively simple measures, including multifactor authentication, network segmentation and endpoint protection. If you have just experienced a breach, it's okay to ask for help from experts. Hire a third party to review your posture, conduct a compromise assessment and work with the team to bolster your defenses and prevent future attacks. **Caleb Barlow, CynergisTek**

5. Use automated adversary simulation tools.

I advise all tech execs who have experienced a devastating attack to learn from their mistakes and take a threat-informed approach to their security strategy moving forward. By using an automated adversary emulation platform to continuously verify security control effectiveness against common adversary methods, organizations will achieve an overall improvement in their security program's outcomes. **Stephan Chenette, AttackIQ**

6. Develop best practices for all tech-related tasks.

My tip in dealing with a major system hack is both simple and complex. Develop explicit procedures addressing best practices around everything from email to social media (the easy part). Engage in user training so that security awareness, response and prevention are part of the corporate mindset (the tough part). Since perps today are more than one step ahead, none of us really has any choice. **Adam Stern, Infinitely Virtual**

7. Educate your employees.

It may sound simple, but it's education. IT leaders once believed their most significant vulnerability was technology, but today most know it's their people. The omnichannel access companies give employees provides opportunities for hackers. To keep our team educated, we use KnowBe4. Based on the employee test attacks we run, KnowBe4 has dramatically of improved our security posture. **Denis King, Solace**

8. Think outside the box.

No book can replace the hands-on experience gained during abnormal activities such as a hack. Learn everything you can about the compromise and think outside the box for a solution that complements the Open Systems Interconnection model—but make it your own by adding a machine vision strategy. **Garry Drummond, LOCH Technologies, Inc.**

9. Leverage nested, distinct security solutions.

There is no single magic bullet for preventing a cyberattack. A defense-in-depth strategy is essential if you're to avoid being a victim. The best way to create layers of defense is to implement a series of nested cybersecurity solutions with as little commonality as possible. If your protections fail differently, it is much more likely that you can prevent or at least survive most attacks. **John Prisco, Safe Quantum Inc.**

10. Invest in external penetration testing.

I would always advocate investing in high-quality external penetration testing as a service. This should quickly highlight the areas of strength and those with potential vulnerabilities, which will steer initial focus and investments in mitigation. **Al Kingsley, NetSupport Limited**

11. Prioritise business continuity and disaster recovery planning.

Make establishing a business continuity and disaster recovery plan a top priority. System hacks and security breaches are a reality in today's world—even with so-called best measures and tighter controls—and it's very important to have a backup system in place in case of an attack to ensure continuity. Disaster recovery already includes measures such as corrective action. **Vishwas Sutar, Lowry Solutions**