Attackers can leverage a compromised email/password combination connected to a **Google account** (such as username@gmail.com) to nefariously install a readily-available message mirroring app on a victim’s smartphone via Google Play.

97% of employees know what constitutes a strong password, yet 53% admit to not always using one.

85% of employees are reusing passwords across business applications after receiving training, in contrast to 91% of employees who haven’t received any cybersecurity training.

Source: https://www.helpnetsecurity.com/2021/08/16/employees-reusing-personal-passwords/
T-Mobile is warning that a data breach has exposed the names, date of birth, Social Security number and driver’s license/ID information of more than 40 million current, former or prospective customers who applied for credit with the company.

The acknowledgment came less than 48 hours after millions of the stolen T-Mobile customer records went up for sale in the cybercrime underground.

Source: https://krebsonsecurity.com/2021/08/t-mobile-breach-exposed-ssn-dob-of-40m-people/?s=09
To help protect US national security, the White House on May 12, 2021, issued Presidential Executive Order (EO) 14028 on Improving the Nation’s Cybersecurity. This EO mandates “significant investments” to help protect against malicious cyber threats.

Section 3 of the EO required federal agencies to develop a plan to adopt a Zero Trust Architecture.

This IR8286 series document is intended to help organizations better implement cybersecurity risk management (CSRM) as an integral part of ERM – both taking its direction from ERM and informing it.

NISTIR 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*

Source: [https://csrc.nist.gov/publications/detail/nistir/8286a/draft](https://csrc.nist.gov/publications/detail/nistir/8286a/draft)
Phases
1. Planning phase
2. IT audit scope and objective
3. Evaluating collected evidence
4. Documenting audit results

IT Security Audit Methodology
1. IT controls
2. General control audit
3. Application control audit
4. Internet and network controls
5. IT Audit standards

Tools for IT audit methodology

A notorious hacking group, known as Shiny Hunters, is reportedly selling a database containing private details of 70 million AT&T customers. However, AT&T, an American telecommunication provider denied suffering from a data breach.

Data stolen include name, contact numbers, physical addresses, social security numbers (SSN), and dates of birth.

Sources: https://www.ehackingnews.com/2021/08/private-details-of-70m-at-users-offered.html?m=1
The Poly Network group said its promise to reward “Mr. White Hat” with a $500,000 bounty still stands, and even invited the hacker to become its “chief security advisor.”

Poly Network said it “has no intention of holding Mr. White Hat legally responsible” for the hack.
Since 2017, five separate Chinese threat groups have used ShadowPad, an infamous Windows backdoor that allows attackers to download additional harmful modules or steal data. In a detailed overview of the malware, SentinelOne researchers Yi-Jhen Hsieh and Joey Chen said that "adoption of ShadowPad significantly reduces the costs of development and maintenance for threat actors," adding that "some threat groups stopped developing their own backdoors after they gained access to ShadowPad."

Source: https://www.ehackingnews.com/2021/08/shadowpad-malware-is-being-sold.html?m=1
A default permissions settings in Microsoft Power Apps might have exposed data of 38 million users’ online, cyber security researchers reported.

The types of data included personal information used for Covid-19 contact tracing, vaccination appointments, social security numbers for job applicants, employee IDs, and millions of names and email addresses.

The vulnerability can be exploited during the device setup process by clicking a link in the License Agreement page that is loaded with **SYSTEM** capabilities. It is not essential to have an authentic SteelSeries device to exploit the problem.

Google, which has announced to invest $10 billion over the next five years to strengthen cybersecurity in the US, said that the governments and businesses are at a watershed moment in addressing cybersecurity.

The company has also pledged, through the Google Career Certificate programme, to train 100,000 Americans in fields like IT support and data analytics, learning in-demand skills including data privacy and security.

About 15 terabytes of police data are missing besides the 7.5 terabytes initially thought to be lost after an information technician inadvertently deleted 22 terabytes of crime data.

The lost data included images, video, audio, case notes and other information gathered by police officers and detectives.
The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added single-factor authentication to the short list of "exceptionally risky" cybersecurity practices that could expose critical infrastructure as well as government and the private sector entities to devastating cyberattacks.

Source: https://thehackernews.com/2021/08/cisa-adds-single-factor-authentication.html
This device may not be the newest wireless router on the block, it’s almost five years old now, but it is a very popular one. A best-seller and recipient of an Amazon’s Choice label in the U.K. store, the TP-Link AC1200 Archer C50 (v6) is cheap and highly recommended by Amazon reviewers. So, what’s not to like?

The FBI has published a private industry advisory, alerting the food and agriculture sectors that they have been under active attack by ransomware organizations. The cybercriminals' approach to firms in this area is unremarkable; the methods and procedures they deploy are well-known.

The Wawa convenience store chain is paying out up to $9 million in cash and gift cards to customers who were affected by a previous data breach, as reimbursements for their loss and inconvenience.

However, the claimants will be required to submit proof of the purchase they conducted at a Wawa store or fuel pump between March 04, 2019, and December 12, 2019 – when the data breach occurred.

The Lightning to USB-C cable used by hackers is made to mimic an Apple cord from the outside. However, it has an accessible interface, one-click payloads, remote Wifi access, and a Keylogger Edition cable that can store up to 650,000 keystrokes.

Source: https://www-thesun-co-uk.cdn.ampproject.org/c/s/www.thesun.co.uk/tech/phones-gadgets/16077289/warning-o-mg-iphone-charging-cable/amp/
Investigators/the FBI/ransomware negotiators just screw everything up, the ransomware gang said, threatening to publish files if victims look for help.

All that the FBI/ransomware negotiators/investigators do is muck things up, so we’re going to publish your stuff if you call for help, the Ragnar Locker ransomware gang announced on its darknet data-leak site.

Angry protests, technological glitches and a plummet in value marked the first day of El Salvador adopting Bitcoin as legal tender. The price of Bitcoin on crashed to its lowest in nearly a month, falling from $52,000 to under $43,000 at one point.

The government has even given Salvadorans $30 each of Bitcoin to encourage its adoption. It says bitcoin could save the country $400m a year in transaction fees on funds sent from abroad.

The End

Prepared By:
Dwight Robinson
www.cyberandrisk.com