ROBERT FRANCES GROUP
Business Advisors to IT Executives

Jul 27, 2020

Summary Insights: Security Gaps and Requirements in New Normal

RFG Perspective: Now that the work-from-home (WFH) environment is settling in as the "New Normal" and will be with us for an extended period of time, a renewed focus needs to be placed on cyberattacks and insider threats. (Twitter hack just one example.) Cybercriminals continue to view COVID-19 as an opportunity for launching new and more deceptive attacks while disgruntled employees are using the loosening of the security guardrails as an opening to extract or tamper with sensitive corporate data and personally identifiable information (PII). Thus, enterprises must re-examine their security policies and procedures to ensure the organization is protected against the significant increase in threats, such as phishing schemes and exploitation of endpoint security gaps.

Introduction

On July 22, 2020, RFG facilitated an RFG 100 Forum videoconference on “the Security Gaps in and Requirements for the New Normal.” Participants included CISOs and top business and IT executives – all of whom are dealing with the security challenges impacting companies that have moved their employees to a work-from-home (WFH) office environment. The panelists on the call were:

- Stan Lowe, Global CISO, zScaler
- Bil Harmer, CISO and Chief Evangelist, SecureAuth
- Malcolm Hawkins, Chief Security and Trust Officer, Cymatic
- Sesh Murthy, CTO, Cloud Raxak
- Mike Davis, CISO, Alliant Group

Although the move to WFH happened rapidly in March, concerns about the New Normal work environment are surfacing. Importantly, the security considerations are getting a second look this summer, as key issues are identified, addressed and remedied.

The biggest security challenges included concerns about email, phishing and social media; administrator errors and the cloud software stack itself. In a quick survey of concerns, the executives highlighted the following as the top ones (see Table 1):

Videoconference (or Event) Survey Results

Table 1: Quick Survey of WFH Security Concerns

The following bullets summarize the key points from the conference call.

Biggest security challenge:

• Email/phishing/social media	78%
• Administrator error	50%
• Cloud	22%
• Web applications	22%

Code vulnerabilities	17%
Networks	11%

Biggest security exposure as a percentage of revenues:

Email/phishing/social media	61%
Malware	50%
Web-based applications	39%
Ransomware	39%
Malicious code	11%
Stolen/lost devices	11%
Botnets	11%
Denial of service	6%

The quick survey simply highlights a longer list of concerns associated with the scramble to move employees into home environments starting in mid-March, 2020 – and extending into April, 2020. Some of the top concerns are associated with building out a more layered security environment that would prevent simple email-related or phishing attacks from compromising corporate security. Other concerns focus on the physical work environment, including concerns about the identity of the people using the remote system – a PC or a laptop – throughout each day's 24-hours of potential use. That is, it's possible that children or visitors could access the remote systems – meaning that two-factor authentication and logging our when taking a break are becoming more important as the COVID-19 crisis rolls into the summer and fall.

Top-of-Mind Concerns for Executives

Following are some top-of-mind comments from the videoconference participants:

- **Risk levels have changed.** The WFH + office environment is not new. It was business-as-usual for most firms prior to the COVID-19 lockdowns. Only the volumes changed as we entered the COVID-19 era. One way to feel comfortable with the level of risk caused by this environment is to use a Web portal for screening and employ VDI for the rest.

- **Personal identity must be verified regarding keyboard access.** Companies will not know who is at a keyboard throughout a 24-hour period. Therefore, continuous authorization is needed. There should be different IDs for each persona. Then companies can use behavioral analytics and credentials to monitor each persona. **Possible solution:** There should be different IDs for each persona. Then companies can use behavioral analytics and credentials to monitor each persona.

- **Who's really in control?** Organizational alignment should be considered – with security awareness and training. Security should be performing behavior analytics on so-called "God credentials," which should give higher security and higher freedoms to users. People take more risks if they believe someone is protecting them. Thus, users must be educated on what is being done and be aware of the tools. More tracking and internal risk assessments -- with a focus on insider risks -- have been implemented. Cyber hygiene is being applied, especially in terms of BYOD (bring your own device). Code vulnerability scanning, using the NIST vulnerability definitions and tools, is another requirement for ensuring that appropriate levels of security software is in place.

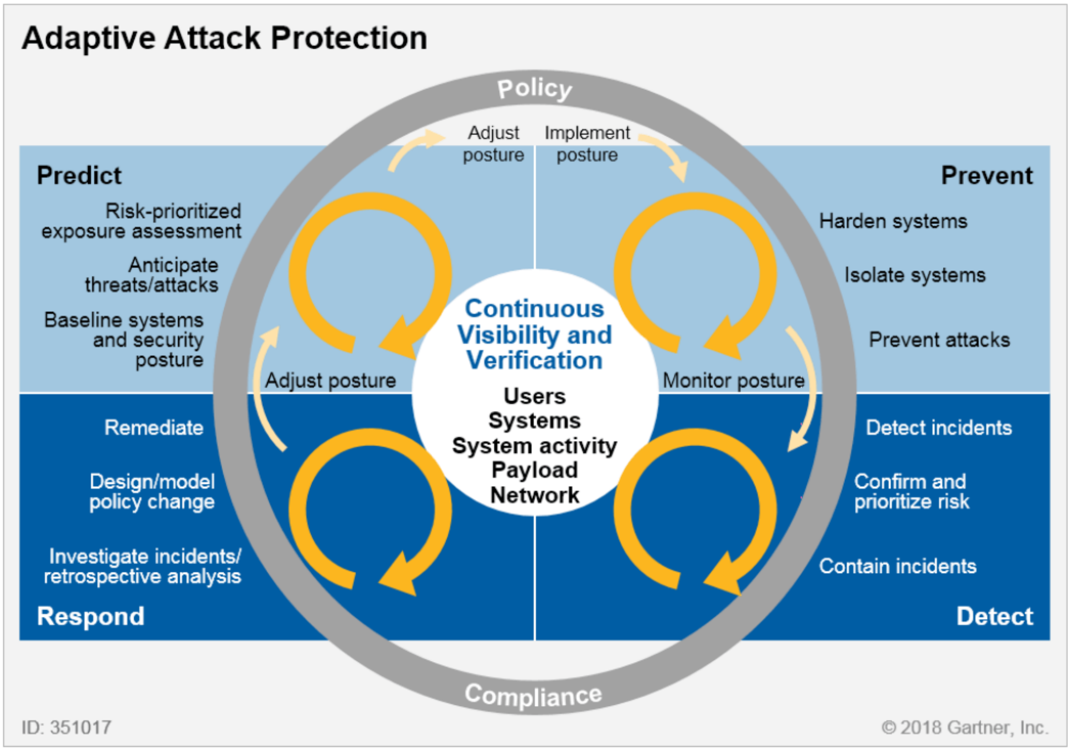
- **What did you know – and when did you know it?** Users of corporate systems must be educated on the firm's risk posture. People take more risks if they believe someone is protecting them. Organizations must ensure that users are being educated about what is being done top safeguard security, across the organization – and they must be made aware of the tools that protect and monitor security levels.

- **Testing your HA/DR and Business Continuity Plans.** Now that we're living with COVID-19 and financial crises, worldwide, incident response plans and BC plans must be reviewed, tested and tested frequently, to ensure they work in case of outages.

- **Security teams must find new ways to monitor employees' actions – even in WFH conditions.** Before the COVID-19 crisis, security personnel regarded themselves as first movers and innovators. Because they, too, are working from home (WFH), security teams may no longer feel like they are leading the security effort. That, in turn, may compromise their ability to manage risk as well as they did in the pre-COVID business environment. Security should consider revisiting this, to ensure that security policies are adhered to.

- **Increasing physical security for workstations, desktops and laptops.** Outsourcing to IT personnel in other countries (e.g., India, the Philippines, Taiwan) brings another level of challenge, now that the work is no longer protected by the physical security of being housed in "safe rooms" and the protocols are suspended. To address this operational challenge to security, many firms have intentionally limited the display of personal information (PII) to the data that is minimally required. Continuous monitoring has been added as well as frequent swapping of individuals or teams working on fixing problems or writing code.

- **Best practices: Ensuring security throughout the New Normal.** New government regulations are coming. They will be based upon the FedRAMP standards for U.S. security software. Many customers consider FedRAMP High to be expensive, so it is likely that the new standards being developed will be based upon FedRAMP Low. In addition, "zero trust" business practices using the Gartner CARTA (continuous adaptive risk and trust) model is also being considered or used.


Adaptive Attack Protection
Policy
Adjust posture
Implement posture
Predict
Risk-prioritized exposure assessment
Anticipate threats/attacks
Baseline systems and security posture
Prevent
Harden systems
Isolate systems
Prevent attacks
Adjust posture
Monitor posture
Continuous Visibility and Verification
Users
Systems
System activity
Payload
Network
Remediate
Design/model policy change
Investigate incidents/ retrospective analysis
Respond
Detect incidents
Confirm and prioritize risk
Contain incidents
Detect
Compliance
ID: 351017
© 2018 Gartner, Inc.

Source: Gartner (April 2018)

- One of the added challenges in large enterprises is that they have deep pockets and therefore not developing their own security solutions but buying them. Therefore they do not know how the security product works – thereby exposing them to product code flaws.

- Security MSPs could add another level of concern for cross-organizational security. If they are now under financial stress as solutions get less expensive, their long-term cash flow and business viability may be called into question, which could impact their ongoing effectiveness. Enterprises are exposed to the MSP's shortfalls and their supply chain. Unfortunately, as some executives observed, there is no MSP CVE to evaluate.

Summary

While the WFH environment is not new, how it is being used today as the primary workstation for most office employees is new and has created additional security gaps that did not exist before the COVID-19 crisis. The rapid move to the WFH situation loosened some long-term guardrails that must now be re-established before the risk exposure becomes worse.

RFG POV: Enterprises cannot become complacent and must take a new look at security policies and procedures to ensure that their risk exposures still fall within acceptable limits. Defense is a game one never wins, but without it, loss is certain. Enterprises must be proactive. Business and IT executives should create a task force to examine their New Normal risk exposures and be prepared to report the results and action items to senior management, including the auditors and board of directors if needed.

Additional relevant research and consulting services are available. Interested readers should contact Client Services to arrange further discussion or interview with Mr. Cal Braunstein, CEO and Executive Director of Research. Jean S. Bozman, President of Cloud Architects Advisors llc, contributed to this report.