SmartFocus on Cybersecurity

A SmartBrief Update

SPONSORED BY American Military University AMU

FALL 2019

HOW TO ADDRESS EVOLVING CYBERSECURITY THREATS

Investing in specialized education is good business

Cybersecurity deserves your attention, whether you are a leader trying to safeguard your enterprise or a professional planning your next career move.

Matthew Gardiner, Director of Security Marketing for email security company Mimecast, explains why.

"Cyberthreats have steadily become more targeted. Attackers, who are primarily interested in making money, have recognized that their return on effort and investment is often best met by researching their intended targets and hitting them for relatively high-impact attacks," he says. "They are going where the money is, which tends to be organizations with valuable data and systems, but perhaps not the best security defenses." And the tactics are more mature and industrialized.

"The most dangerous cyberattackers are not individual actors, but often part of an attacker supply chain, where the profits are divided much like a legitimate corporation would with its ecosystem," he continues. "To support this, attacker groups have become specialized, with some providing technical tooling, others providing hosting, others conducting campaign execution, and still others providing fencing services and financial payments management."

HARMFUL THREATS ABOUND

The three most common and costly threats, according to data from the FBI's Internet Crime Complaint Center are:

1 PERSONAL DATA BREACHES

"Companies realize that these lapses in security cost more than bad press — they cost millions in liability, loss of customers and market share," says Colleen Madden Blumenfeld of Challenger, Gray & Christmas. "Meanwhile, many jurisdictions across the country are passing legislation that compels companies to alert customers and vendors when any sort of breach occurs." Last year alone, hackers gained access to the personal data of millions of people, creating losses of $148,892,403, according to the FBI.

2 EXTORTION

In this tactic, cyberextortionists threaten the release of sensitive data or intimidate with financial or physical harm to coerce victims to hand over something of value. It grew 242% from 2017 to 2018 and affected 51,146 victims.

3 EMAIL COMPROMISE

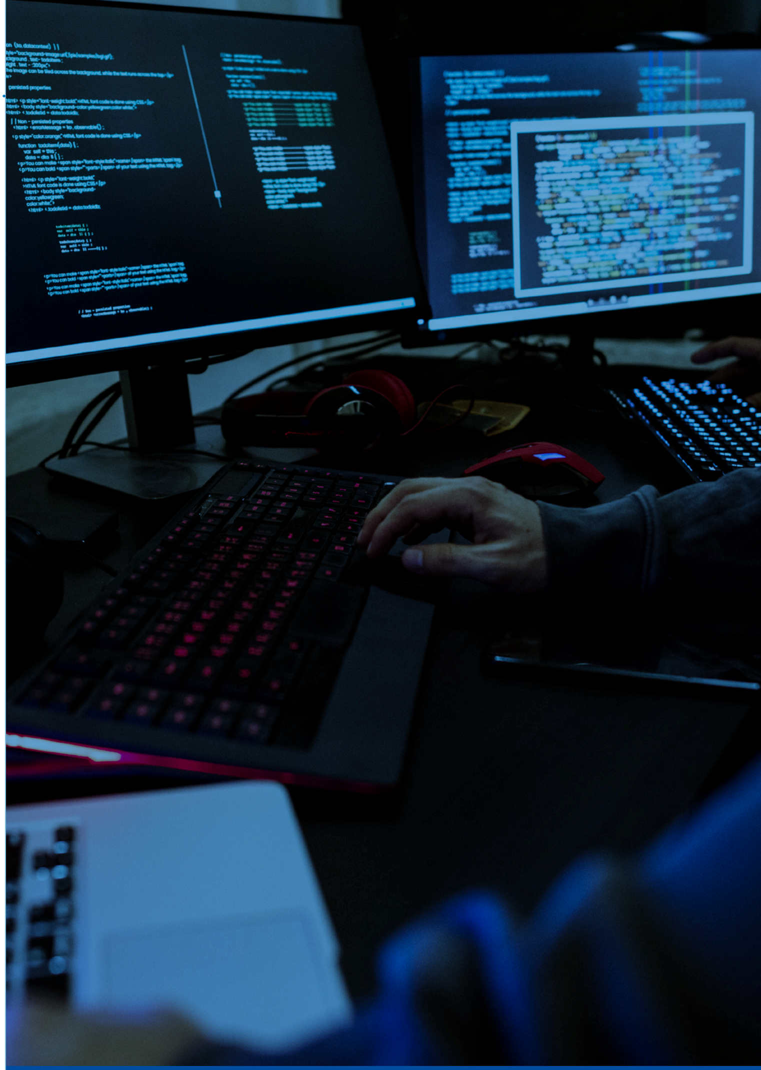
"Email security represents only about 2% of security spend overall, but the vast majority of attacks leverage email," Gardiner notes. "Given the rate at which email-borne attacks are working, more attention is warranted." In 2018, the FBI received 20,373 Business Email Compromise/ Email Account Compromise complaints, producing losses in excess of $1.2 billion.

EVOLVING THREATS INVOLVE NEW TACTICS

Cybercrime advances as quickly as technology does. Here are three emerging tactics to watch.

1 ARTIFICIAL INTELLIGENCE

From deep fakes to AI-generated phishing emails, cybercriminals leverage artificial intelligence to make it easier to get what they want. They are even using AI to train datasets used in machine learning. By deploying this approach, cyberthieves could modify data designed to detect malware, so it marks the dangerous code as clean.



> "The most dangerous cyberattackers are not individual actors, but often part of an attacker supply chain, where the profits are divided much like a legitimate corporation would with its ecosystem."
>
> — **MATTHEW GARDINER,** *Director of Security Marketing, Mimecast*

2 INTERNET OF THINGS

The usefulness of connected devices, wearable technologies and smart homes is convenient, but comes with a cost, according to Dr. Kevin Harris, Program Director for Cybersecurity, Information Systems Security and Information Technology Management at American Military University. "IoT, while improving conveniences, has increased the threat vector for cyberattacks and must be effectively secured prior to implementation to avoid widespread access for cyberattackers."

3 BREAKING ENCRYPTION

According to a new report by the National Academies of Sciences, Engineering and Medicine, today's encryption could be decoded by quantum computers in the not-too-distant future. Why worry now? Because it will take longer to build and install algorithms to protect against encryption-breaking than it will to build a computer that can crack the code.

Being unaware of and unprepared for these threats puts your organization at risk and that requires a new way of looking at cyberprotection.

Learn more about cyberthreats at InCyberDefense.com.

> “Users are literally the last line of defense against many types of cyberattacks, in particular email-borne ones.”
>
> — **MATTHEW GARDINER,**
> *Director of Security Marketing, Mimecast*

KEY CHALLENGE: ADDRESSING THE SKILLS SHORTAGE IN CYBERSECURITY

With record-low unemployment and strong competition for workers — especially technical workers — organizations struggle to attract and retain a skilled workforce.

According to a recent survey of 150 HR executives at companies nationwide from Challenger, Gray & Christmas, 82% of companies are hiring, 32% of those are looking for IT/network/software workers and 70% report a skills shortage.

Adding to the shortage: Immigration reforms that slash H-1B visas supporting IT staffing needs. "Tech companies especially have warned legislators that changes to these work visas is costing them skilled talent they cannot find in the U.S.," Blumenfeld reports.

No wonder 45% of respondents to the Duke Global Business Outlook survey said identifying, hiring and keeping talent was their No. 1 issue.

PROTECTING YOUR ORGANIZATION

Safeguarding your enterprise from cyberhackers and other bad actors requires focused tactics.

- **Make cybersecurity an executive- and board-level priority.** "Security is not primarily an IT problem," Gardiner asserts. "It's a business problem, a risk management problem. The risk tolerance of the organization needs to be considered and then investments in security need to be applied accordingly." When cybersecurity becomes a strategic issue for the organization's top decision-makers, employees and job candidates see and follow the commitment.
- **Upgrade HR practices to focus on identifying and recruiting candidates with cybersecurity credentials, and integrate cybersecurity into onboarding.** Blumenfeld says that as more companies are going to a data-driven performance model, workers in marketing, finance and compliance will need to be able to collect and analyze key performance indicators and use existing tech to spur growth.

EDUCATION REDUCES RISKS FROM CYBERTHREATS

"Making the decision to pursue studies in cybersecurity allows individuals to not only gain technical competencies but understand the impact of cyberthreats against organizations as well as how to effectively present material to a diverse audience," notes Dr. Kevin Harris, Program Director for Cybersecurity, Information Systems Security and Information Technology Management for American Military University.

CONSIDER THESE OPTIONS:

- Associate degree programs provide specific skill sets often required in the cybersecurity industry and prepare learners for related bachelor's programs.
- Bachelor's programs are an option for those seeking a strong theoretical conceptual discipline understanding and technical knowledge of their field of study.
- Graduate degrees are suitable for people to distinguish themselves from their peers in leadership roles.
- Certificate programs, at the bachelor's and master's levels, also offer pathways for cybersecurity professionals to continue lifelong learning and stay ahead of emerging cyberthreats and learn new protocols and best practices.

"Whether you're military or nonmilitary, American Military University has a diverse set of online degree and certificate programs allowing individuals to select a program that fits their personal and professional goals," he adds.

Learn more about cybersecurity education at American Military University. ■

- **Provide ongoing staff training at regular intervals.** "Users are literally the last line of defense against many types of cyberattacks, in particular email-borne ones," Gardiner notes. "The more aware and cautious staff can be, the less likely they will fall for common attacks and the more likely they will report suspicious activities to the security team. This is why security awareness training is so key to a security program."

- **Engage employees in other functional areas.** IT security departments are well-positioned to be the owner of the overall cybersecurity program, but not the exclusive owner, Gardiner states. "The risk management of the organization should include all departments that have a hand in managing the associated risk: executives, HR, IT, legal, finance, sales and IT security."

- **Invest in continuing education for current staff.** Providing or subsidizing corporate training, workshops and seminars and degree programs is an important tactic for addressing the skills shortage and subverting cybercrime. "If companies cannot find the talent needed, they will have to foster it," Blumenfeld explains.

"Cybersecurity is a large and varied area," concludes Dr. Ahmed Naumaan, Dean of the School of Science, Technology, Engineering and Math at American Military University. "Consequently, it is important for everyone to study cybersecurity to some extent; and, of course, given the extensive demand for employees in the cybersecurity sector, studying it in depth is a great option." ■

> Cybersecurity is a large and varied area… Consequently, it is important for everyone to study cybersecurity to some extent; and, of course, given the extensive demand for employees in the cybersecurity sector, studying it in depth is a great option.
>
> — **DR. AHMED NAUMAAN,**
> *Dean of the School of Science, Technology, Engineering and Math, American Military University*

ABOUT AMERICAN MILITARY UNIVERSITY (AMU)

Founded by a Marine Corps officer to provide military personnel with portable, relevant, and affordable education, American Military University is a leading provider of higher education to the U.S. military, with a reach that extends to veterans, national security, intelligence, public safety, and other mission-driven professionals. With a student population exceeding 80,000, AMU offers more than 200 online degree and certificate programs. Our working adult students gain leading edge knowledge in critical areas, such as cybersecurity, intelligence studies, homeland security, and emergency and disaster management, as they learn from faculty who are practitioners in their field and hold distinguished academic credentials.

Learn more at:
AMUonline.com/cybersecurity

sponsored by

AMU American Military University