Atlantic Council

PRESENTS:

IT TAKES A VILLAGE:

HOW HACKTIVITY CAN SAVE YOUR COMPANY

Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

ABOUT US

THE SCOWCROFT CENTER FOR STRATEGY AND SECURITY works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

THE ATLANTIC COUNCIL'S CYBER STATECRAFT INITIATIVE is housed within the Scowcroft Center for Strategy and Security. The focus of the Initiative is to: (1) examine the nexus of geopolitics and national security with cyberspace; (2) continue to build out the new field of cyber safety in the Internet of Things; and (3) help build the next generation of cybersecurity and cyberspace policy professionals. Throughout all of its work, the Initiative focuses relentlessly on providing practical, innovative, and relevant solutions to challenges in cyberspace. The Initiative brings together a diverse network of respected experts, bridging the gap between the technical and policy communities.

THE INITIATIVE IS ENGAGED IN THIS PROJECT out of its commitment to convening technologists and policymakers to develop actionable and technically literate policy solutions to secure the future together. Coordinated Vulnerability Disclosure (CVD) is an accepted cybersecurity best practice in mitigating cyber threats by enlisting the support of outside actors and security researchers in reporting software or application vulnerabilities. Despite its resounding success, CVD still faces many challenges. With this comic, we hope to promote better understanding of CVD practices among policymakers and business leaders, as well as the misperception of CVD as a catch-all solution for cybersecurity threats.

IT TAKES A VILLAGE: HOW HACKTIVITY CAN SAVE YOUR COMPANY

AUTHOR: SHAUN EE

ILLUSTRATOR: MEREDITH GRAN

SHAUN EE is a program assistant with the Atlantic Council's Asia Security Initiative and Cyber Statecraft Initiative within the Scowcroft Center for Strategy and Security. Prior to joining the Council, Shaun graduated from Washington University in St. Louis with a BA in international studies and neuroscience.

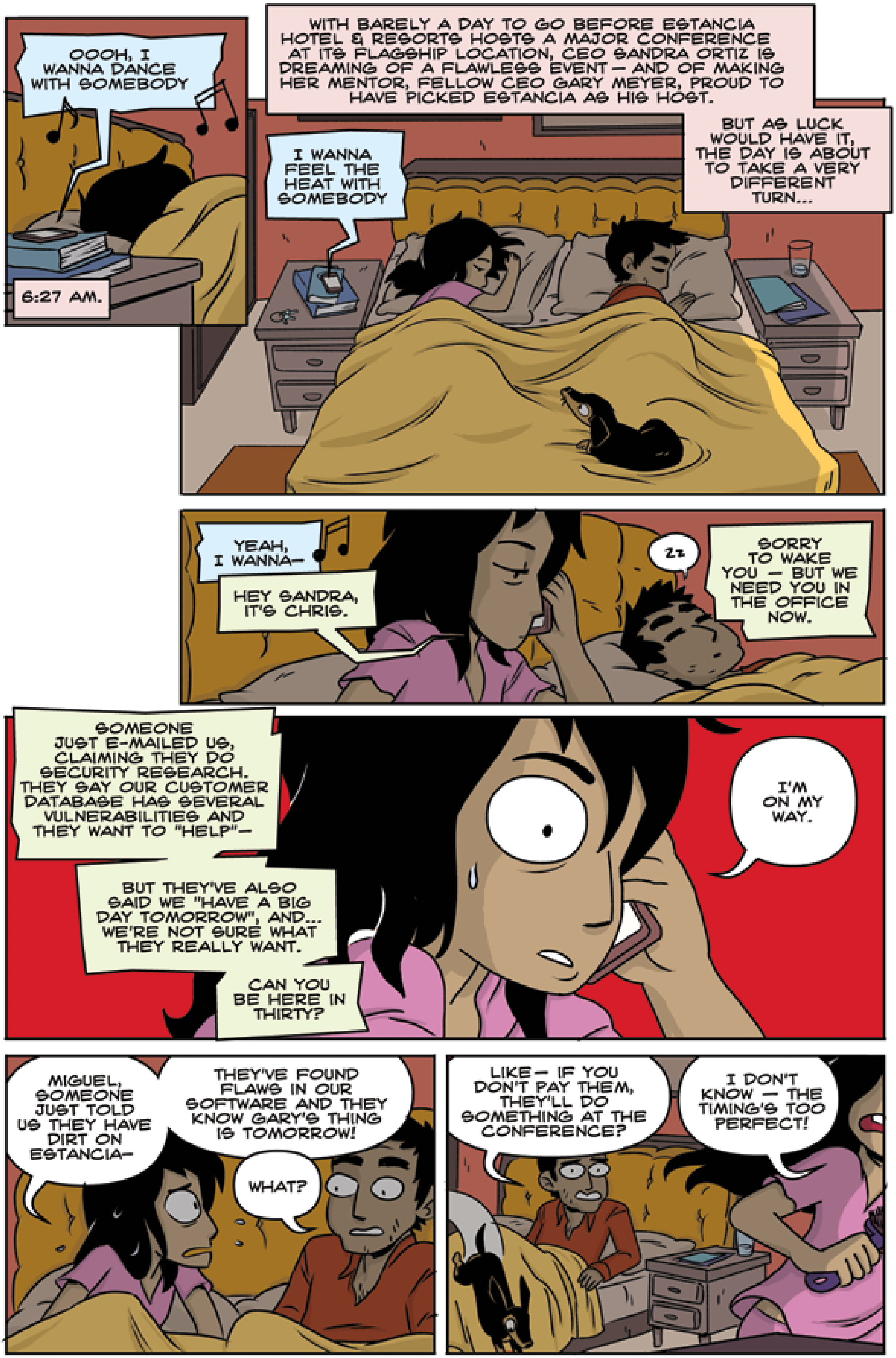
MEREDITH GRAN is the cartoonist and animator behind the popular web comic *Octopus Pie*, as well as the Adventure Time comic series *Marceline and the Scream Queens*. She lives in Philadelphia, PA and teaches comics at the School of Visual Arts.

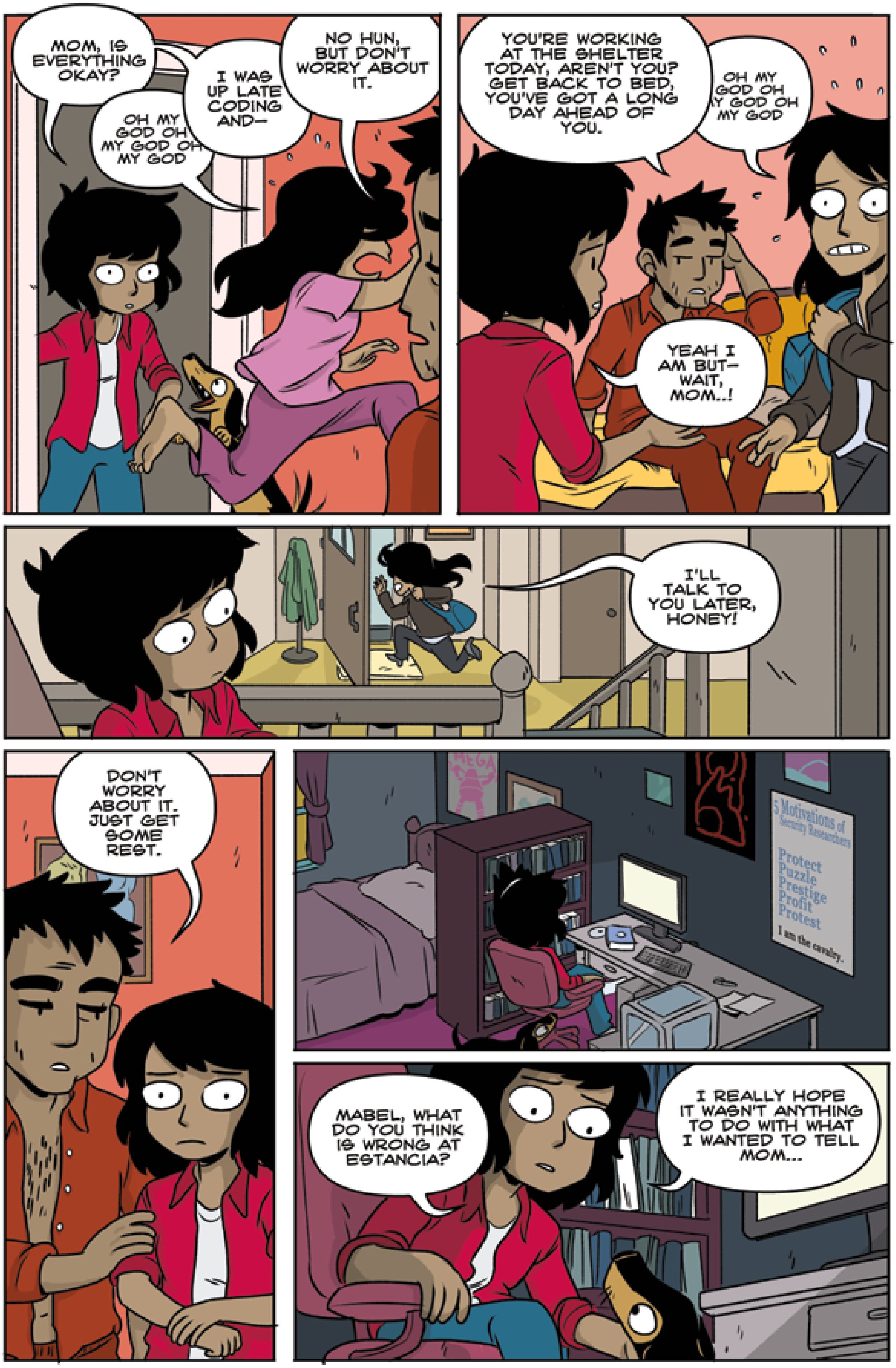
ACKNOWLEDGEMENTS:

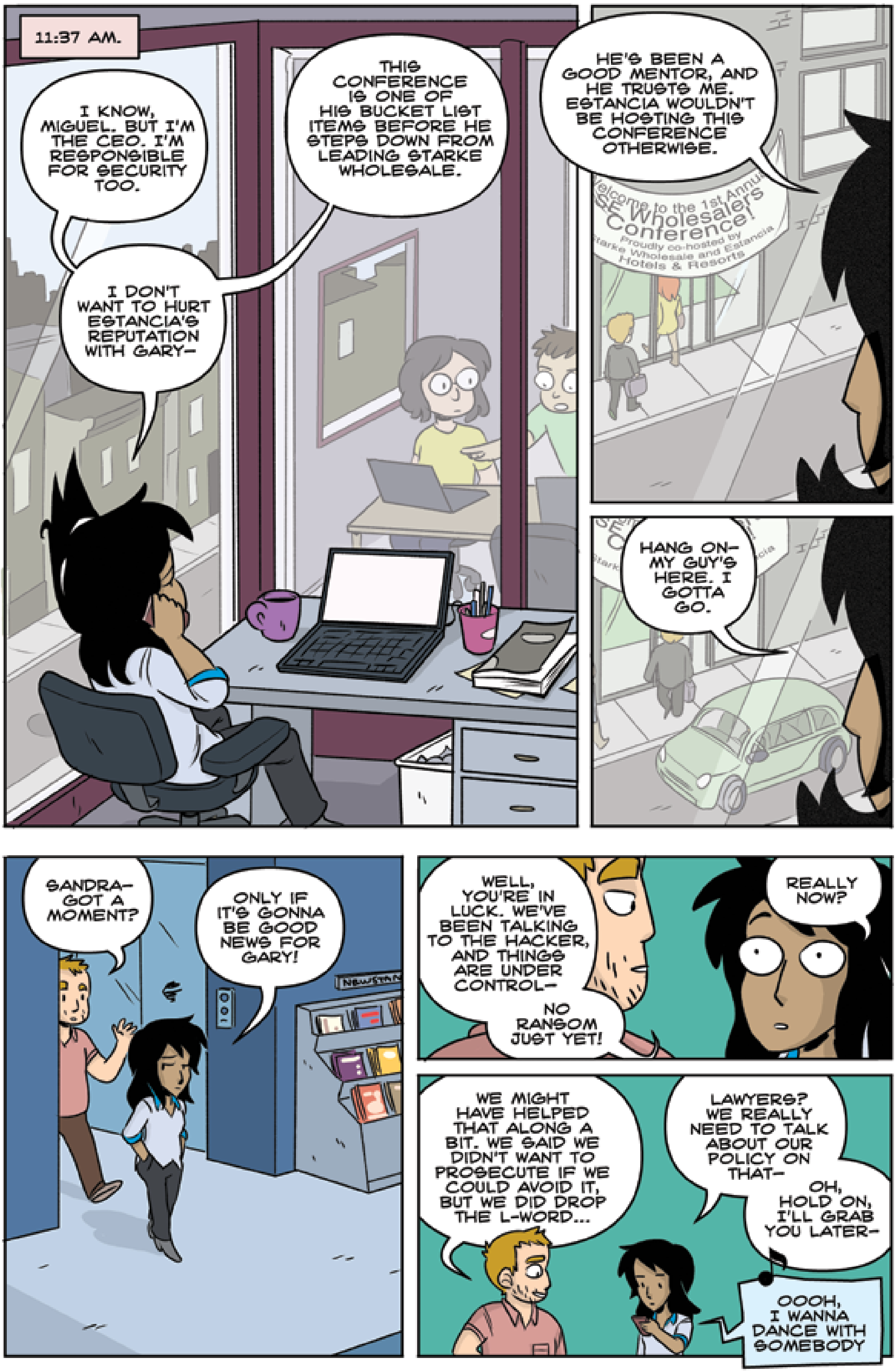
Thank you to HackerOne for their generous support for this project, allowing the Cyber Statecraft Initiative to tackle a challenging topic in the field of cybersecurity in a way that is not only fun, but emphasizes the human side of those who work in the interest of keeping us safe. A special thanks to our senior fellow Beau Woods for his invaluable insights into the security research community, and to the Atlantic Council team that made this all possible, especially Klara Jordan, Safa Shahwan, Heather Regnault, Anca Agachi, and Timothy McGiff.

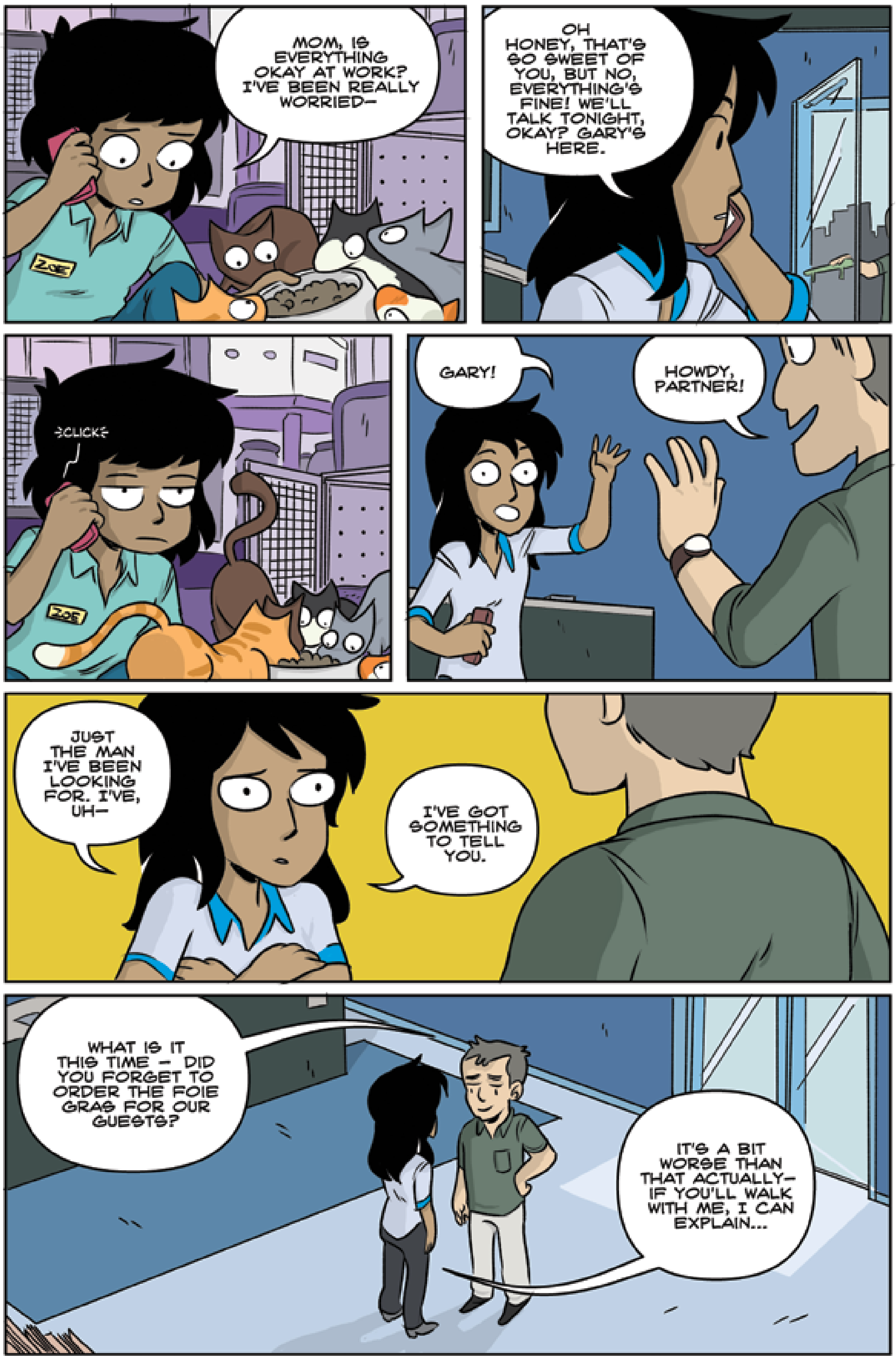
ISBN-13: 978-1-61977-563-3

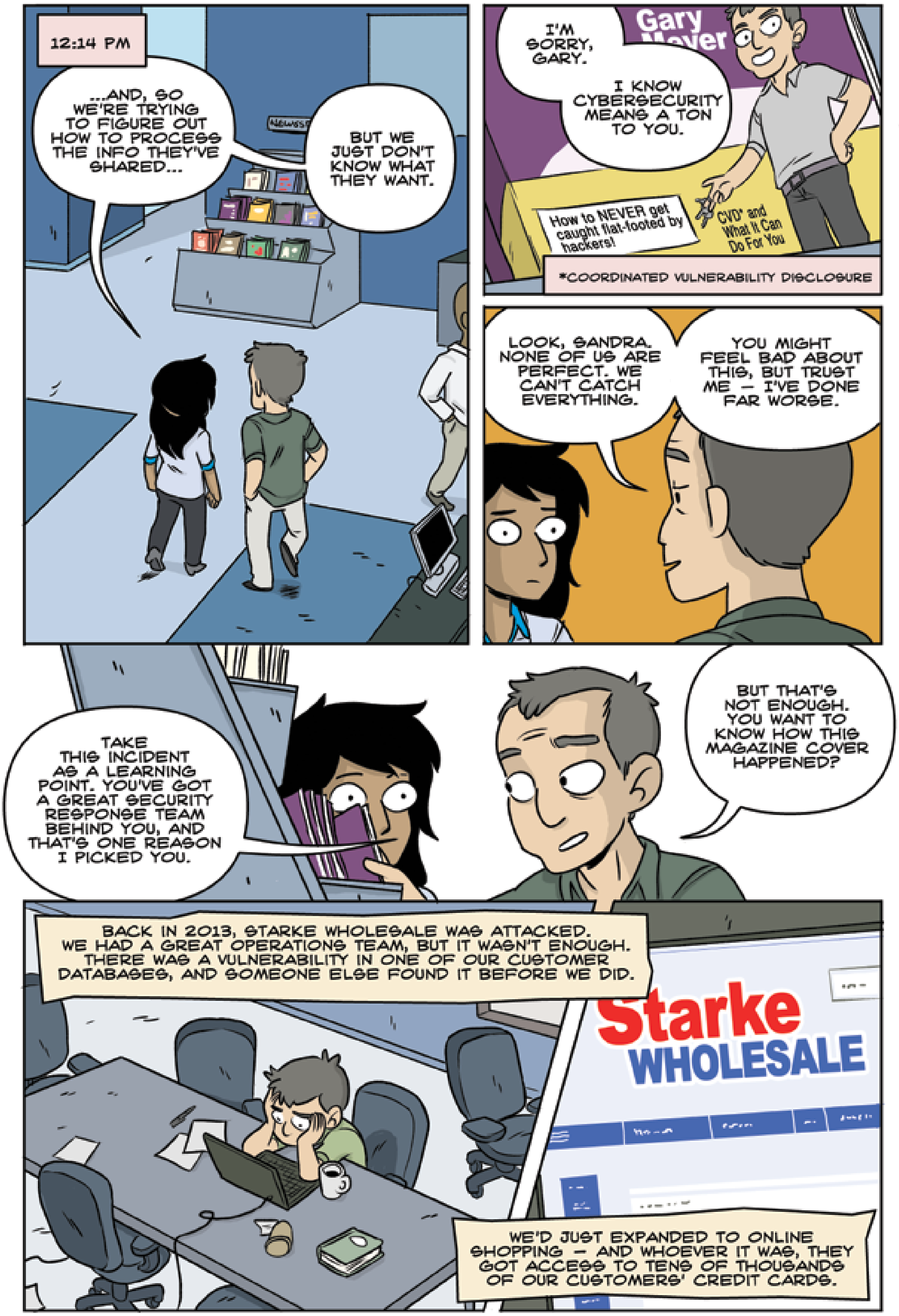
This report is written and published in accordance with the Atlantic Council policy on intellectual independence. The authors are solely responsible for its analysis and recommendations. The Atlantic Council and its donors do not determine, nor do they necessarily endorse or advocate for, any of this report's conclusions.

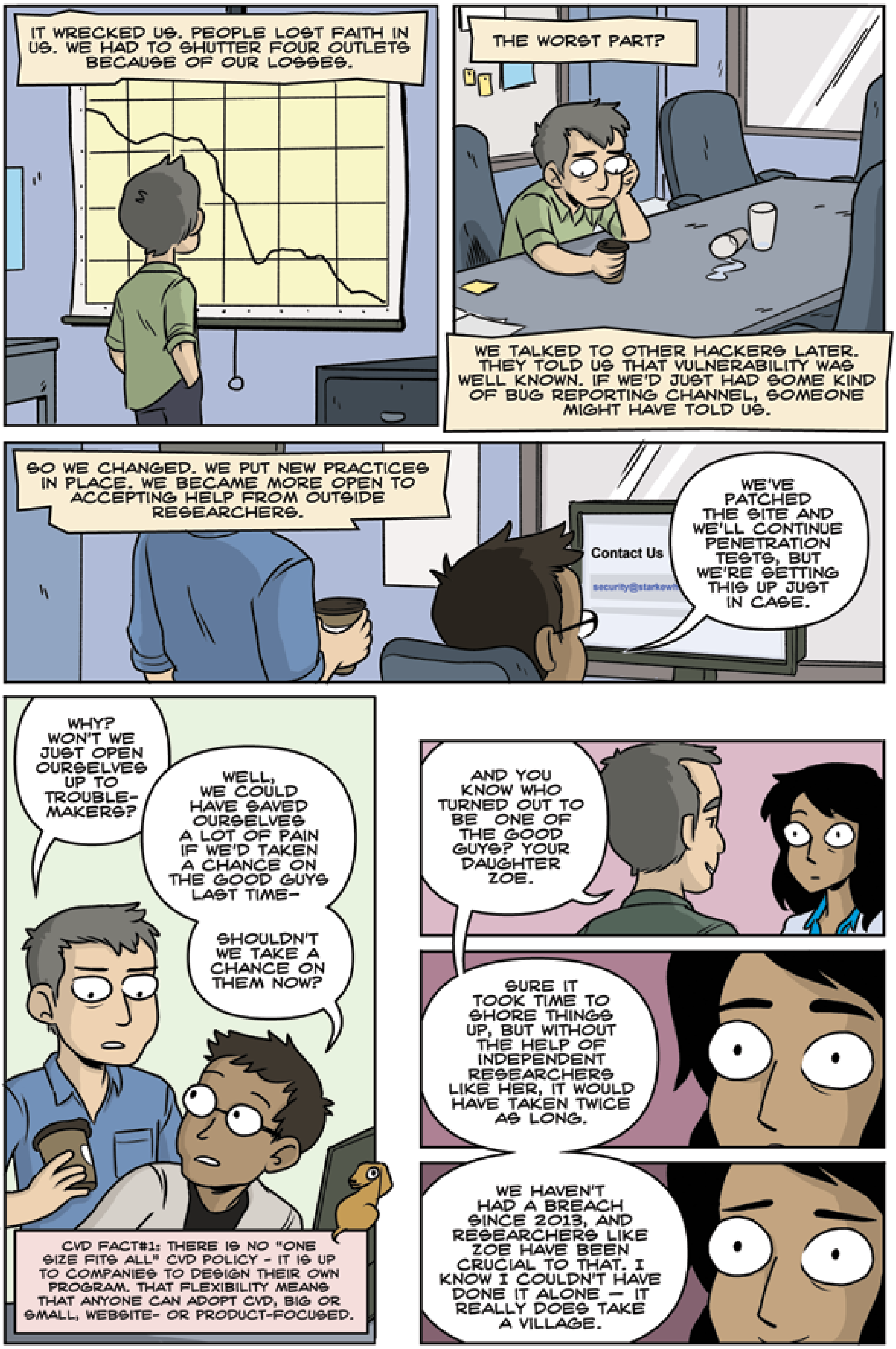

OOOH, I WANNA DANCE WITH SOMEBODY
6:27 AM.
WITH BARELY A DAY TO GO BEFORE ESTANCIA HOTEL & RESORTS HOSTS A MAJOR CONFERENCE AT ITS FLAGSHIP LOCATION, CEO SANDRA ORTIZ IS DREAMING OF A FLAWLESS EVENT — AND OF MAKING HER MENTOR, FELLOW CEO GARY MEYER, PROUD TO HAVE PICKED ESTANCIA AS HIS HOST.
I WANNA FEEL THE HEAT WITH SOMEBODY
BUT AS LUCK WOULD HAVE IT, THE DAY IS ABOUT TO TAKE A VERY DIFFERENT TURN...
YEAH, I WANNA—
HEY SANDRA, IT'S CHRIS.
ZZ
SORRY TO WAKE YOU — BUT WE NEED YOU IN THE OFFICE NOW.
SOMEONE JUST E-MAILED US, CLAIMING THEY DO SECURITY RESEARCH. THEY SAY OUR CUSTOMER DATABASE HAS SEVERAL VULNERABILITIES AND THEY WANT TO "HELP"—
BUT THEY'VE ALSO SAID WE "HAVE A BIG DAY TOMORROW", AND... WE'RE NOT SURE WHAT THEY REALLY WANT.
CAN YOU BE HERE IN THIRTY?
I'M ON MY WAY.
MIGUEL, SOMEONE JUST TOLD US THEY HAVE DIRT ON ESTANCIA—
THEY'VE FOUND FLAWS IN OUR SOFTWARE AND THEY KNOW GARY'S THING IS TOMORROW!
WHAT?
LIKE— IF YOU DON'T PAY THEM, THEY'LL DO SOMETHING AT THE CONFERENCE?
I DON'T KNOW — THE TIMING'S TOO PERFECT!

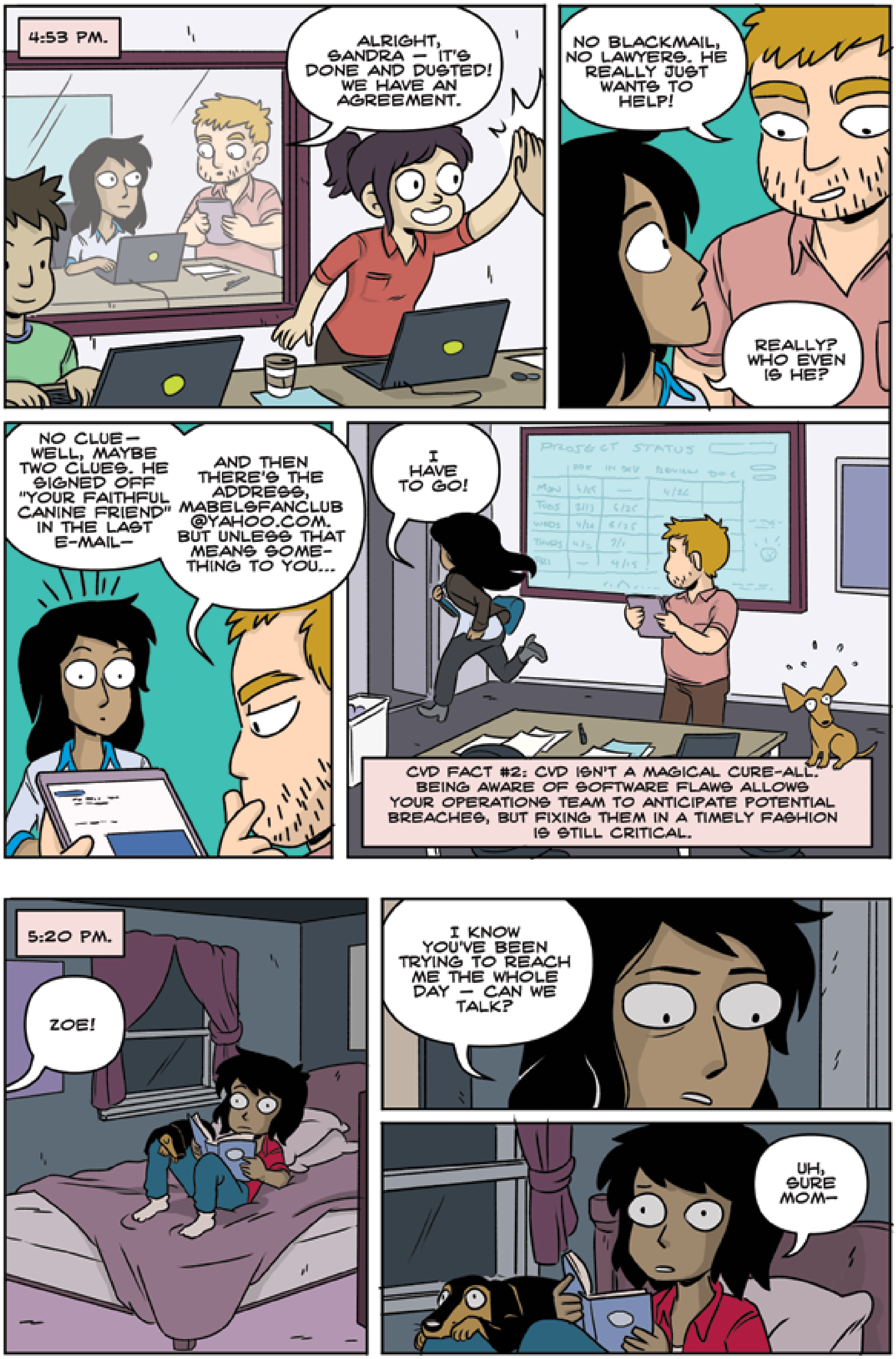

MOM, IS EVERYTHING OKAY?
OH MY GOD OH MY GOD OH MY GOD
I WAS UP LATE CODING AND–
NO HUN, BUT DON'T WORRY ABOUT IT.
YOU'RE WORKING AT THE SHELTER TODAY, AREN'T YOU? GET BACK TO BED, YOU'VE GOT A LONG DAY AHEAD OF YOU.
OH MY GOD OH MY GOD OH MY GOD
YEAH I AM BUT– WAIT, MOM..!
I'LL TALK TO YOU LATER, HONEY!
DON'T WORRY ABOUT IT. JUST GET SOME REST.
MEGA
5 Motivations of Security Researchers
Protect
Puzzle
Prestige
Profit
Protest
I am the cavalry.
MABEL, WHAT DO YOU THINK IS WRONG AT ESTANCIA?
I REALLY HOPE IT WASN'T ANYTHING TO DO WITH WHAT I WANTED TO TELL MOM...

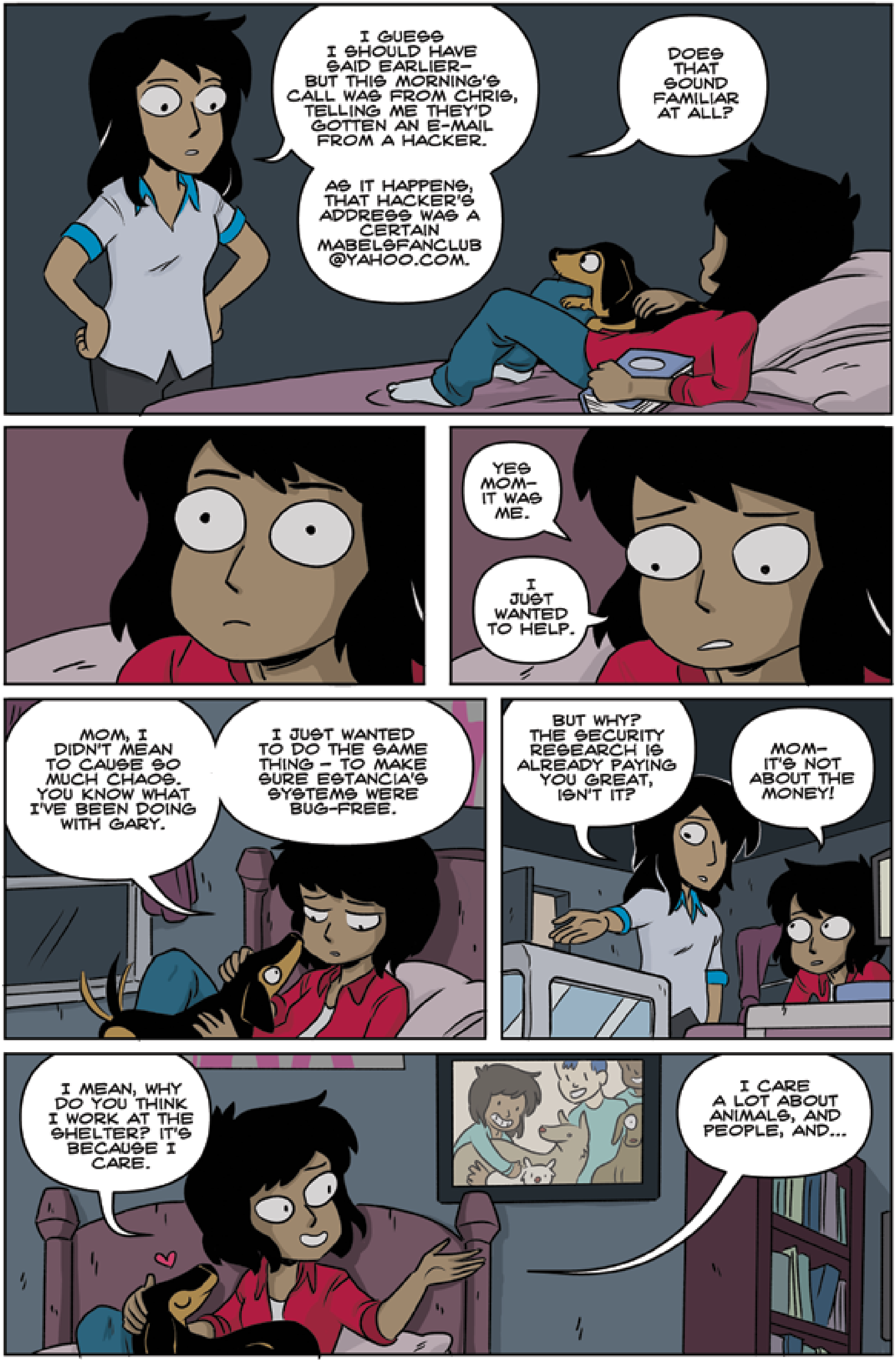

11:37 AM.
I KNOW, MIGUEL. BUT I'M THE CEO. I'M RESPONSIBLE FOR SECURITY TOO.
I DON'T WANT TO HURT ESTANCIA'S REPUTATION WITH GARY–
THIS CONFERENCE IS ONE OF HIS BUCKET LIST ITEMS BEFORE HE STEPS DOWN FROM LEADING STARKE WHOLESALE.
HE'S BEEN A GOOD MENTOR, AND HE TRUSTS ME. ESTANCIA WOULDN'T BE HOSTING THIS CONFERENCE OTHERWISE.
Welcome to the 1st Annu
SE Wholesalers Conference!
Proudly co-hosted by Starke Wholesale and Estancia Hotels & Resorts
HANG ON– MY GUY'S HERE. I GOTTA GO.
SANDRA– GOT A MOMENT?
ONLY IF IT'S GONNA BE GOOD NEWS FOR GARY!
NEWSSTAN
WELL, YOU'RE IN LUCK. WE'VE BEEN TALKING TO THE HACKER, AND THINGS ARE UNDER CONTROL–
NO RANSOM JUST YET!
REALLY NOW?
WE MIGHT HAVE HELPED THAT ALONG A BIT. WE SAID WE DIDN'T WANT TO PROSECUTE IF WE COULD AVOID IT, BUT WE DID DROP THE L-WORD...
LAWYERS? WE REALLY NEED TO TALK ABOUT OUR POLICY ON THAT–
OH, HOLD ON, I'LL GRAB YOU LATER–
OOOH, I WANNA DANCE WITH SOMEBODY

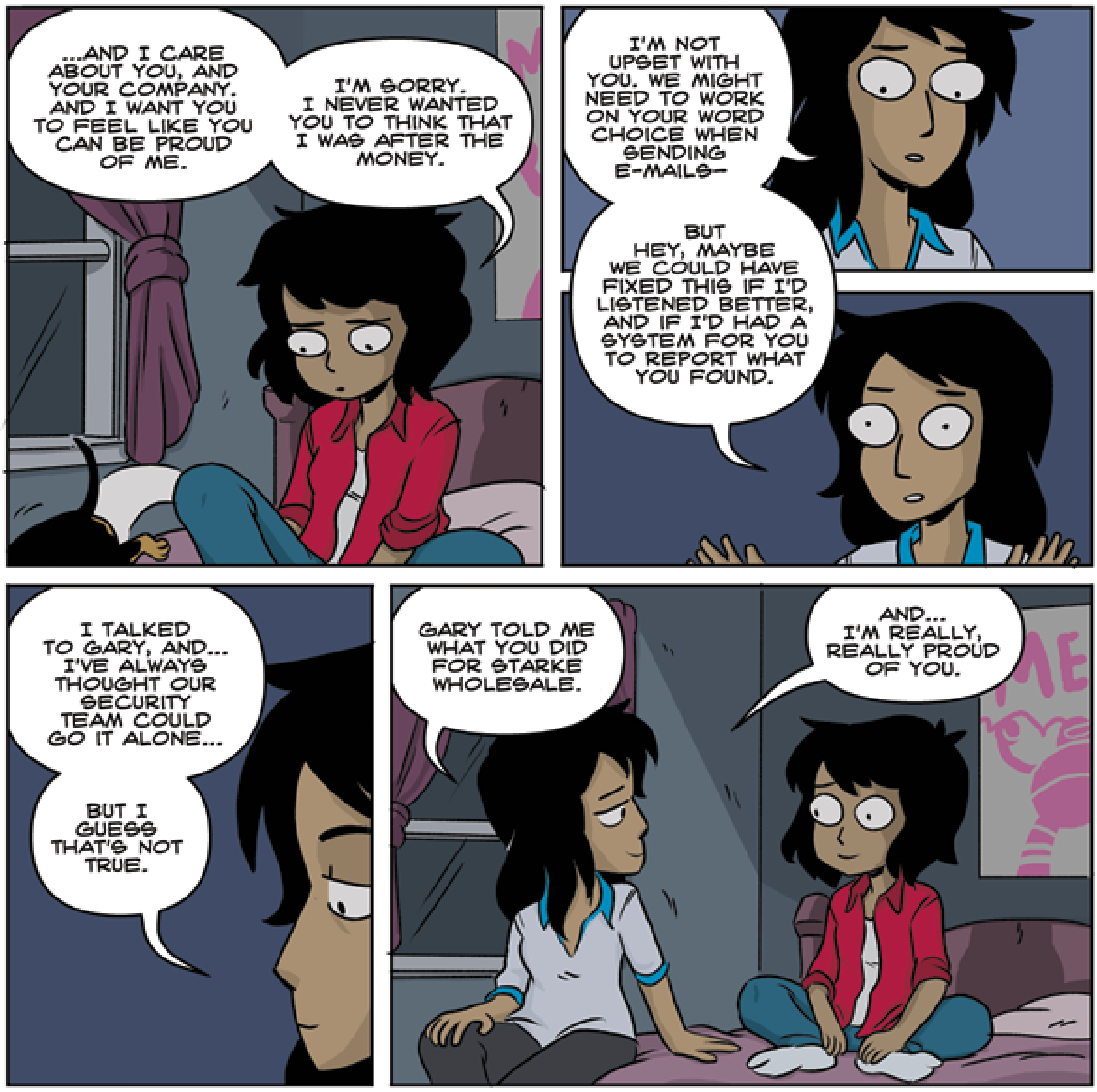

ZOE
MOM, IS EVERYTHING OKAY AT WORK? I'VE BEEN REALLY WORRIED—
OH HONEY, THAT'S SO SWEET OF YOU, BUT NO, EVERYTHING'S FINE! WE'LL TALK TONIGHT, OKAY? GARY'S HERE.
ZOE
≶CLICK≷
GARY!
HOWDY, PARTNER!
JUST THE MAN I'VE BEEN LOOKING FOR. I'VE, UH—
I'VE GOT SOMETHING TO TELL YOU.
WHAT IS IT THIS TIME — DID YOU FORGET TO ORDER THE FOIE GRAS FOR OUR GUESTS?
IT'S A BIT WORSE THAN THAT ACTUALLY— IF YOU'LL WALK WITH ME, I CAN EXPLAIN...


12:14 PM
...AND, SO WE'RE TRYING TO FIGURE OUT HOW TO PROCESS THE INFO THEY'VE SHARED...
BUT WE JUST DON'T KNOW WHAT THEY WANT.
I'M SORRY, GARY.
I KNOW CYBERSECURITY MEANS A TON TO YOU.
Gary Meyer
How to NEVER get caught flat-footed by hackers!
CVD* and What It Can Do For You
*COORDINATED VULNERABILITY DISCLOSURE
LOOK, SANDRA. NONE OF US ARE PERFECT. WE CAN'T CATCH EVERYTHING.
YOU MIGHT FEEL BAD ABOUT THIS, BUT TRUST ME — I'VE DONE FAR WORSE.
TAKE THIS INCIDENT AS A LEARNING POINT. YOU'VE GOT A GREAT SECURITY RESPONSE TEAM BEHIND YOU, AND THAT'S ONE REASON I PICKED YOU.
BUT THAT'S NOT ENOUGH. YOU WANT TO KNOW HOW THIS MAGAZINE COVER HAPPENED?
BACK IN 2013, STARKE WHOLESALE WAS ATTACKED. WE HAD A GREAT OPERATIONS TEAM, BUT IT WASN'T ENOUGH. THERE WAS A VULNERABILITY IN ONE OF OUR CUSTOMER DATABASES, AND SOMEONE ELSE FOUND IT BEFORE WE DID.
Starke WHOLESALE
WE'D JUST EXPANDED TO ONLINE SHOPPING — AND WHOEVER IT WAS, THEY GOT ACCESS TO TENS OF THOUSANDS OF OUR CUSTOMERS' CREDIT CARDS.

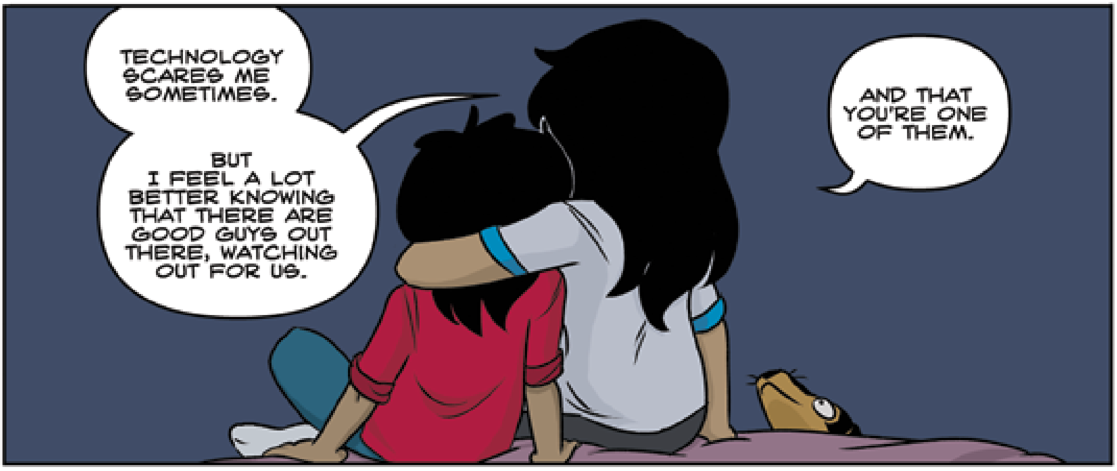

IT WRECKED US. PEOPLE LOST FAITH IN US. WE HAD TO SHUTTER FOUR OUTLETS BECAUSE OF OUR LOSSES.
THE WORST PART?
WE TALKED TO OTHER HACKERS LATER. THEY TOLD US THAT VULNERABILITY WAS WELL KNOWN. IF WE'D JUST HAD SOME KIND OF BUG REPORTING CHANNEL, SOMEONE MIGHT HAVE TOLD US.
SO WE CHANGED. WE PUT NEW PRACTICES IN PLACE. WE BECAME MORE OPEN TO ACCEPTING HELP FROM OUTSIDE RESEARCHERS.
Contact Us
security@starkew
WE'VE PATCHED THE SITE AND WE'LL CONTINUE PENETRATION TESTS, BUT WE'RE SETTING THIS UP JUST IN CASE.
WHY? WON'T WE JUST OPEN OURSELVES UP TO TROUBLE-MAKERS?
WELL, WE COULD HAVE SAVED OURSELVES A LOT OF PAIN IF WE'D TAKEN A CHANCE ON THE GOOD GUYS LAST TIME–
SHOULDN'T WE TAKE A CHANCE ON THEM NOW?
CVD FACT#1: THERE IS NO "ONE SIZE FITS ALL" CVD POLICY - IT IS UP TO COMPANIES TO DESIGN THEIR OWN PROGRAM. THAT FLEXIBILITY MEANS THAT ANYONE CAN ADOPT CVD, BIG OR SMALL, WEBSITE- OR PRODUCT-FOCUSED.
AND YOU KNOW WHO TURNED OUT TO BE ONE OF THE GOOD GUYS? YOUR DAUGHTER ZOE.
SURE IT TOOK TIME TO SHORE THINGS UP, BUT WITHOUT THE HELP OF INDEPENDENT RESEARCHERS LIKE HER, IT WOULD HAVE TAKEN TWICE AS LONG.
WE HAVEN'T HAD A BREACH SINCE 2013, AND RESEARCHERS LIKE ZOE HAVE BEEN CRUCIAL TO THAT. I KNOW I COULDN'T HAVE DONE IT ALONE — IT REALLY DOES TAKE A VILLAGE.


4:53 PM.
ALRIGHT, SANDRA — IT'S DONE AND DUSTED! WE HAVE AN AGREEMENT.
NO BLACKMAIL, NO LAWYERS. HE REALLY JUST WANTS TO HELP!
REALLY? WHO EVEN IS HE?
NO CLUE— WELL, MAYBE TWO CLUES. HE SIGNED OFF "YOUR FAITHFUL CANINE FRIEND" IN THE LAST E-MAIL—
AND THEN THERE'S THE ADDRESS, MABELSFANCLUB@YAHOO.COM. BUT UNLESS THAT MEANS SOMETHING TO YOU...
I HAVE TO GO!
PROJECT STATUS
CVD FACT #2: CVD ISN'T A MAGICAL CURE-ALL. BEING AWARE OF SOFTWARE FLAWS ALLOWS YOUR OPERATIONS TEAM TO ANTICIPATE POTENTIAL BREACHES, BUT FIXING THEM IN A TIMELY FASHION IS STILL CRITICAL.
5:20 PM.
ZOE!
I KNOW YOU'VE BEEN TRYING TO REACH ME THE WHOLE DAY — CAN WE TALK?
UH, SURE MOM—


I GUESS I SHOULD HAVE SAID EARLIER– BUT THIS MORNING'S CALL WAS FROM CHRIS, TELLING ME THEY'D GOTTEN AN E-MAIL FROM A HACKER.
AS IT HAPPENS, THAT HACKER'S ADDRESS WAS A CERTAIN MABELSFANCLUB @YAHOO.COM.
DOES THAT SOUND FAMILIAR AT ALL?
YES MOM– IT WAS ME.
I JUST WANTED TO HELP.
MOM, I DIDN'T MEAN TO CAUSE SO MUCH CHAOS. YOU KNOW WHAT I'VE BEEN DOING WITH GARY.
I JUST WANTED TO DO THE SAME THING – TO MAKE SURE ESTANCIA'S SYSTEMS WERE BUG-FREE.
BUT WHY? THE SECURITY RESEARCH IS ALREADY PAYING YOU GREAT, ISN'T IT?
MOM– IT'S NOT ABOUT THE MONEY!
I MEAN, WHY DO YOU THINK I WORK AT THE SHELTER? IT'S BECAUSE I CARE.
I CARE A LOT ABOUT ANIMALS, AND PEOPLE, AND...


...AND I CARE ABOUT YOU, AND YOUR COMPANY. AND I WANT YOU TO FEEL LIKE YOU CAN BE PROUD OF ME.
I'M SORRY. I NEVER WANTED YOU TO THINK THAT I WAS AFTER THE MONEY.
I'M NOT UPSET WITH YOU. WE MIGHT NEED TO WORK ON YOUR WORD CHOICE WHEN SENDING E-MAILS—
BUT HEY, MAYBE WE COULD HAVE FIXED THIS IF I'D LISTENED BETTER, AND IF I'D HAD A SYSTEM FOR YOU TO REPORT WHAT YOU FOUND.
I TALKED TO GARY, AND... I'VE ALWAYS THOUGHT OUR SECURITY TEAM COULD GO IT ALONE...
BUT I GUESS THAT'S NOT TRUE.
GARY TOLD ME WHAT YOU DID FOR STARKE WHOLESALE.
AND... I'M REALLY, REALLY PROUD OF YOU.

CVD FACT #3: NOT ALL CVD PROGRAMS INVOLVE BUG BOUNTIES. ETHICAL HACKERS OFTEN AREN'T IN IT FOR THE MONEY - THEY'RE THERE TO PROTECT CYBER SAFETY AND THE COMMON GOOD.


TECHNOLOGY SCARES ME SOMETIMES.
BUT I FEEL A LOT BETTER KNOWING THAT THERE ARE GOOD GUYS OUT THERE, WATCHING OUT FOR US.
AND THAT YOU'RE ONE OF THEM.

WANT TO GO SEE WHAT'S FOR DINNER?
CVD SHOULD BE A CRUCIAL PART OF ANY COMPANY'S CYBERSECURITY STRATEGY, NO MATTER HOW BIG OR SMALL.
CVD IS PAINLESS TO SET UP -- IT CAN BE JUST ONE NEW E-MAIL ADDRESS AWAY. BUT IT BOLSTERS YOUR DEFENSES ENORMOUSLY, AND FOR VERY LITTLE COST.
SOMETIMES, WE HAVE INCREDIBLE RESOURCES RIGHT UNDER OUR NOSE. CVD LETS US TAP INTO THEIR EXPERTISE.
REMEMBER -- WE ARE ALL ON THE SAME SIDE AGAINST CYBER INSECURITY.

TO: chris@estancia.org

Chris -- let's look into how to write up a CVD policy...

YOU ARE NOT ALONE.

A LITTLE ON COORDINATED VULNERABILITY DISCLOSURE PROGRAMS

With our modern-day reliance on digital technology, software and system vulnerabilities have become increasingly hard to avoid. Left unchecked, malicious actors can exploit them to compromise systems and damage public trust. Thoroughly eliminating all these vulnerabilities can be a challenge, but CVD programs allow governments and private companies to mitigate them alongside independent security researchers, working together to create a more secure digital ecosystem.

Through a CVD program, members of the security research community can contact organizations and vendors about vulnerabilities that they find in their products, systems, and configurations, giving them time to deploy a fix before those vulnerabilities become public knowledge. When instituted and followed, a CVD program allows companies to manage the process of disclosure and handling of vulnerabilities in a controlled fashion by working with security researchers to coordinate a set of common terms and a timeline. This way, companies can avoid surprises while keeping their customers and systems safe.

Unlike bug bounty programs, CVD programs do not always involve paying security researchers, many of whom are just looking to mitigate vulnerabilities of systems or software or hoping to be recognized for their work. Nonetheless, it is still possible (but not necessary) to establish a CVD program by working with outside entities that help coordinate vulnerability reports.

Cyber insecurity affects every aspect of our lives, from how we work to how we travel or how we vote. Grappling with those issues can be overwhelming at times, but CVD empowers us to tackle them together. **Remember—we are all on the same side against cyber insecurity. You are not alone.**

SOME MOTIVATIONS OF HACKERS[1]

PROTECT – make the world a safer place. These researchers are drawn to problems where they feel they can make a difference.

PUZZLE – tinker out of curiosity. This type of researcher is typically a hobbyist and is driven to understand how things work.

PRESTIGE – seek pride and notability. These researchers often want to be the best, or very well known for their work.

PROFIT – to earn money. These researchers trade on their skills as a primary or secondary income.

PROTEST/PATRIOTISM – ideological and principled. These researchers, whether patriots or protestors, strongly support or oppose causes.

SOME FACTS ABOUT CVD

FACT #1: There is no "one size fits all" CVD policy—it is up to companies to design their own program. That flexibility means that anyone can adopt CVD, big or small, website- or product-focused.

FACT #2: CVD isn't a magical cure-all. Being aware of software flaws allows your operations team to anticipate potential breaches, but fixing them in a timely fashion is still critical.

FACT #3: Not all CVD programs involve bug bounties. Ethical hackers often aren't in it for the money—they're there to protect cyber safety and the common good.

FIND OUT MORE ABOUT CVD HERE:

Angela Simpson, "Improving Cybersecurity Through Enhanced Vulnerability Disclosure," National Telecommunications and Information Administration, December 15, 2016, https://www.ntia.doc.gov/blog/2016/improving-cybersecurity-through-enhanced-vulnerability-disclosure.

Allen D. Householder, Garret Wasserman, Art Manion, and Chris King, "The CERT Guide to Coordinated Vulnerability Disclosure," Carnegie Mellon University Software Engineering Institute, August 2017, https://insights.sei.cmu.edu/cert/2017/08/the-cert-guide-to-coordinated-vulnerability-disclosure.html.

[1] "5 Motivations of Security Researchers," *I Am the Cavalry,* retrieved September 10, 2018, https://www.iamthecavalry.org/motivations.

Atlantic Council

THE ATLANTIC COUNCIL IS A NONPARTISAN ORGANIZATION THAT PROMOTES CONSTRUCTIVE US LEADERSHIP AND ENGAGEMENT IN INTERNATIONAL AFFAIRS BASED ON THE CENTRAL ROLE OF THE ATLANTIC COMMUNITY IN MEETING TODAY'S GLOBAL CHALLENGES.

ATLANTIC COUNCIL

1030 15TH STREET, NW, 12TH FLOOR,
WASHINGTON, DC 20005

(202) 463-7226, WWW.ATLANTICCOUNCIL.ORG